You've been hacked!
Cyber threats, A.I., Security and Attorney Ethical Obligations

Theodore Roosevelt American Inn of Court
Hybrid: At Nassau County Bar Association & By Zoom
March 20, 2024

Presented by: Hon. Ira Warshawsky
Jess Bunshaft, Esq.
Thomas O'Rourke, Esq.
Byron Chou, Esq.
Elizabeth Daitz, Esq.
Victoria Ciminera, St. John's Law School
Abigail Drummond, St. John's Law School
Asma Halimi, St. John's Law School

<u>Timed Agenda</u>

Introduction Examples of Cyberthreats to Law Firms: 6:00-6:10pm Jess Bunshaft

Skit 1, Preventing Cybersecurity Breaches : 6:10-6:22pm Judge Warshawsky, Elizabeth Daitz, Victoria Ciminera

Additional Examples of Hacks and Presentation NY Ethics Rules : 6:22-6:47pm Elizabeth Daitz, Victoria Ciminera, Abigail Drummond, Asma Halimi

Skit 2, Preventing Cyber Thefts and Ethical Issues in Transactions involving IOLA Accounts. Example-the law firm/real estate transaction: 6:47-6:57pm – Byron Chou, Judge Warshawsky, Tom O'Rourke

Presentation on Artificial Intelligence Issue: 6:57-7:12pm – Byron Chou

Skit 3, Prevention of Malware and Protecting Confidential Client Communications : 7:12-7:20pm Judge Warshawsky, Tom O'Rourke, Abigal Drummond, Victoria Ciminera

Skit 4, Ethical and Cybersecurity Issues in Ransomware Attacks -the hospital: 7:20-7:28pm Elizabeth Daitz, Jess Bunshaft, Asma Halimi, Abigail Drummond, Byron Chou, Judge Warshawsky

Skit 5, Additional scams Attorneys Should be Aware of: 7:28-7:35pm Asma Halimi, Abigail Drummond, Victoria Ciminera

Closing discussion: 7:35-7:43pm

Q&A

Lawyers, Professional Responsibility, & Cybersecurity

New York Rules of Professional Conduct

RULE 1.1

- **COMPETENCE**

  (a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

  (b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

New York Rules of Professional Conduct

RULE 1.1

- **COMPETENCE**

Comment [8] To maintain the requisite knowledge and skill, a lawyer should

(i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice,

(ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and

(iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 NYCRR Part 1500

New York’s Uniform Trial Court Rules

RULE 202.12(b)

Further, counsel for all parties who appear at the preliminary conference must be sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery.

Counsel may bring a client representative or outside expert to assist in such e-discovery discussions.

New York Rules of Professional Conduct

RULE 5.3

Lawyer's Responsibility for Conduct of Nonlawyers

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

New York Rules of Professional Conduct

RULE 1.6

CONFIDENTIALITY OF INFORMATION

1.6 (a) A lawyer shall not

- knowingly reveal confidential information . . . .

1.6(c) A lawyer shall make reasonable efforts

- to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to information protected by Rules 1.6, 1.9(c), or 1.18(b).

New York County Lawyers Association Professional Ethics Committee

Formal Opinion 749

February 21, 2017

Topic: A lawyer’s ethical duty of technological competence with respect to the duty to protect a client’s confidential information from cybersecurity risk and handling e-discovery when representing clients in a litigation or government investigation.

New York County Lawyers Association Professional Ethics Committee

Formal Opinion 749

Compliance with RPC 1.6 requires

- That lawyers who use technology to store or transmit a client's confidential information, or to communicate with clients use **reasonable** care with respect to those uses

Lawyers must have a sufficient understanding of the technology

- Either directly or through associating with persons possessing such knowledge.
- To determine how to satisfy the lawyer's duty of **reasonable** care.

New York County Lawyers Association Professional Ethics Committee

CONCLUSION

A lawyer fulfills his or her duty of competence with respect to technology: if the lawyer possesses the requisite knowledge personally

- acquires the requisite knowledge in a timely manner and before performance is required
- or associates with one or more persons who possess the requisite technological knowledge.
- If a lawyer is unable to satisfy the duty of technological competence associated with a matter, the lawyer should decline the representation.

ABA Formal Opinion 477
Securing Communication of Protected Client Information
(Excerpted)

Provides that it is a “lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the information.”

The Opinion suggests a fact-based approach to your issue.
Guidance to interpret what “reasonable” means in Rule 1.6(c).

Reasonable efforts is not susceptible to a hard and fast rule but is contingent upon a set of factors. Comment [18] to Model Rule 1.6(c) Provides these factors.

Non-exclusive factors to guide lawyers in making a "reasonable efforts" determination.

- **the sensitivity of the information,**
- **the likelihood of disclosure if additional safeguards are not employed,**
- **the cost of employing additional safeguards,**
- **the difficulty of implementing the safeguards, and**
- **the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).**
- **Use these to determine what is reasonable.**

Case By Case Basis Analysis
Factors to Be Considered

1. Understand the Nature of the Threat.
2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.
3. Understand and Use Reasonable Electronic Security Measures.
4. Determine How Electronic Communications About Clients Matters Should Be Protected
5. Label Client Confidential Information.
6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.
7. Conduct Due Diligence on Vendors Providing Communication Technology.

Remember your duty under rule 5.3 to supervise the non-lawyer and to make “reasonable efforts to ensure that” the non-lawyers “conduct is compatible with the professional obligations of the lawyer.”

Factors to Be Considered on the Selection of the Vendor

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Cure Incompetence

Lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.

Comment [3] to Model Rule 5.3 addresses using non-lawyers in rendering legal services to the client.

It includes- "using an Internet-based service to store client information." [The Cloud]

Comment [3] provides that the "reasonable efforts" required by Model Rule 5.3 to ensure that the non-lawyer's services are provided in a manner that is compatible with the lawyer's professional obligations "will depend upon the circumstances."

Cure Incompetence

Factors could Include

- the education, experience, and reputation of the non-lawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information;
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality. [Watch out for Europe]

Conclusion

Generally, a lawyer may transmit information relating to the representation of a client over the internet, without violating the Model Rules of Professional Conduct if the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access.

Conclusion

However, “a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.”

SEC Disclosure Requirements

New Item 1.05 of Form 8-k – “Material Cybersecurity Incidents”

- Describe the nature, scope & timing of the incident & its impact within 4 business days of the material incident (w/ limited exceptions)

Item 1C of Form 10-K – “Cybersecurity”

- Required disclosure of company’s processes for assessing, identifying and managing cybersecurity threats
- Should consider whether the company engages any third parties with their processes, & how to processes how been integrated

These new requirements should prompt public companies to:

(1) Ensure that incident response policies are in place to escalate incidents to leadership

(2) Establish framework for determining materiality without delay after discovery of an incident

(3) Prepare new disclosures for company’s report regarding assessment, identification and management of risks as well if any risks affect business strategy

https://www.corporatecomplianceinsights.com/sec-cybersecurity-rules-details-2023/.

Cyber Insurance

- First Party Coverage
  - The insurer pays the organization’s expenses incurred directly due to a security breach
- Third Party Coverage
  - This policy covers damages or settlements that organization must pay due to suits or claims for injuries resulting from the organization’s actions or failure to take action

https://www.bluevoyant.com/knowledge-center/5-types-of-cyber-insurance-coverage-and-what-to-watch-out-for

What is not covered by Cyber Liability Insurance?

- Poor security processes – attacks that occur as a result of ineffective security processes
- Prior breaches – breaches prior to the purchase of a cyber insurance policy
- Human error – errors caused by the company’s personnel
- Insider attacks – by an employee
- Technology system improvements

https://www.bluevoyant.com/knowledge-center/5-types-of-cyber-insurance-coverage-and-what-to-watch-out-for.

Looking Ahead

2021 Formal Ethics Opinion 2 – North Carolina State Bar – *A Lawyer's Professional Responsibility in Identifying Avoiding Counterfeit Checks* (July 16, 2021)

- Lawyer violated the Rules of Professional Conduct by not investigating the authenticity of a third party, foreign bank's cashier checks – Lawyer should be on alert for potential fraud

NC State bar warns of heightened discipline for wire fraud – "Lawyers who fail to take adequate precautions to protect against wire fraud scams can expect imposition of more serious professional discipline."

https://www.ncbar.org/2021/08/24/heightened-discipline-for-wire-fraud/

Office of the NEW YORK
STATE COMPTROLLER
NYS Comptroller Thomas P. DiNapoli

NEWS from the Office of the New York State Comptroller

Contact: Press Office 518-474-4015

Share

DiNapoli: Cyberattack Complaints in New York Rise 53%

NY's Ransomware and Data Breaches Third Highest in Nation Over Six Years; Over $775 Million Lost in 2022 Alone

October 5, 2023

Cyberattack complaints in New York state increased 53% between 2016 and 2022, jumping from 16,426 incidents in 2016 to 25,112 in 2022, according to the FBI. The number of attacks targeting critical infrastructure in New York state nearly doubled to 83 in the first half of 2023 compared to 48 during the entirety of last year, according to a report released today by State Comptroller Thomas P. DiNapoli.

Estimated losses in New York from cyberattacks in 2022 totaled over $775 million, while losses nationwide totaled $10.3 billion.

“Cyberattacks are a serious threat to New York’s critical infrastructure, economy and our everyday lives,” said DiNapoli. “Data breaches at companies and institutions that collect large amounts of personal information expose New Yorkers to potential invasions of privacy, identity theft and fraud. Also troubling is the rise in ransomware attacks that can shut down systems we rely on for water, power, health care and other necessities. Safeguarding our state from cyberattacks requires sustained investment, coordination, and vigilance."

Relative to other states, New York had the third highest number of ransomware attacks (135) and corporate data breaches (238) in 2022, trailing only California and Texas for ransomware attacks and California and Florida for corporate data breaches. New York also had the fourth-highest number of cybercrime victims in the nation in 2022 with losses skyrocketing 632% since 2016.

The two most attacked critical infrastructure sectors through ransomware and data breaches in New York were Healthcare and Public Health (9) and Financial Services (8). Commercial Facilities and Government Facilities (7) tied for third.

Combatting the Threat

Securing critical infrastructure from cyberattacks will require sustained investment, coordination and vigilance. In 2022, the Governor appointed a state chief cyber officer to lead cross-agency efforts to combat cyber threats and improve the state's critical infrastructure assets' cybersecurity. The cyber chief leads a newly created Joint Security Operations Center, a multi-agency cybersecurity coordination hub linking New York state, New York City, local and regional governments and critical infrastructure stakeholders and federal partners for information sharing, cyber threat detection and incident response. In August, the Governor released the first statewide cybersecurity strategy, which will allow the state to access new federal funding.

The federal Cyber Incident Reporting for Critical Infrastructure Act of 2022, for which rules and regulations are being developed, will require cybersecurity reporting for critical infrastructure sectors. The creation of a centralized repository of data breach reports from across the critical infrastructure sectors would also aid in identifying new attack-vectors or exploits before they become widespread, and for coordinated responses to emerging cyberthreats. Encompassing local governments in this database would be important.

DiNapoli's cybersecurity audits of state agencies and public authorities have found several common technical weaknesses and risks across its audits, such as entities' misunderstanding of security risks, unsupported applications, unknown data on systems, poor access controls and a lack of monitoring of changes to systems, among others. Recommendations are provided to each agency to enable them to begin corrective actions immediately to strengthen their networks.

Cybersecurity Challenges Facing NY's Local Governments and Schools

DiNapoli also released a report on the cybersecurity challenges facing New York's local governments and school districts. In New York, cyberattacks have impacted local governments and schools both large and small, including reported attacks at counties including Albany, Chenango, Erie, Nassau, Schenectady, Suffolk, and Schuyler; cities including New York, Albany, Buffalo, Yonkers, Long Beach, and Olean; and towns including Brookhaven, Ulster, Canandaigua, and Moreau.

In 2019, a ransomware attack on the Syracuse City School District froze the district out of its own systems, crippling the website, email system, phones, and back-end functions like payroll and student management. Other attacks on local governments have had far reaching impacts. The September 2022 ransomware attack on Suffolk County, the ramifications of which the county is still dealing with, required the county to disable important computer systems and move many of the county's functions back to pen and paper for months. It was a cautionary example of the potential impacts of a cyberattack, and highlighted the risk to state systems that linked local government systems could pose.

These and other recent events have demonstrated the serious risks that illegal access to these systems can pose to critical local government and school operations that rely heavily on technology. DiNapoli's report provides guidance and resources for local governments and schools to help them manage the risks associated with cybersecurity.

Risks in Local Governments and School Districts

From 2019 through July 31, 2023, DiNapoli’s Local Government and School Accountability division released more than 190 information technology (IT) audits, finding more than 2,400 cybersecurity-related issues. The audits focused on breakdowns or gaps in fundamental cybersecurity components. The most common areas where improvement and corrective action were needed included cybersecurity governance aspects such as training in IT security awareness, policies and procedures, and the need for contingency plans. Because these cybersecurity audits are sensitive in nature, many findings and recommendations for corrective action are communicated confidentially to local government and school officials. Often the audit recommendations can be implemented at no or low cost to local governments or school districts.

Reports

Cyberattacks on New York’s Critical Infrastructure: Staying Ahead of the Threat

New York Local Government and School Cybersecurity: A Cyber Profile

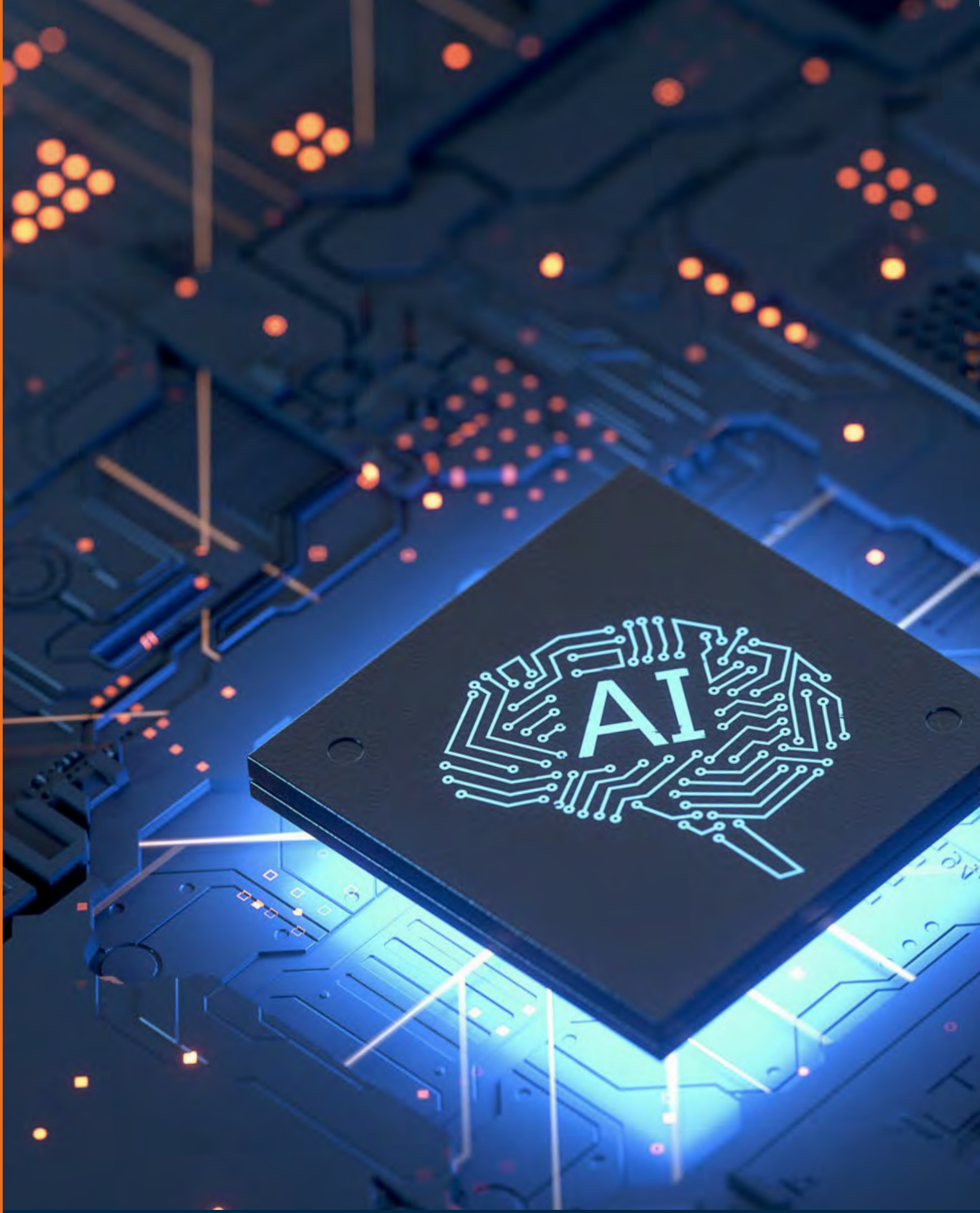
OUR OFFICE

TOOLS

INITIATIVES

HELP

How would you rate our website? ★★★★★



2023
2024

CISA ROADMAP
FOR
ARTIFICIAL INTELLIGENCE

PUBLICATION:
NOVEMBER 2023

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CONTENTS

INTRODUCTION

As noted in the landmark Executive Order 14110, “Safe, Secure, And Trustworthy Development and Use of Artificial Intelligence (AI),” signed by the President on October 30, 2023, “AI must be safe and secure.” As the nation’s cyber defense agency and the national coordinator for critical infrastructure security and resilience, CISA will play a key role in addressing and managing risks at the nexus of AI, cybersecurity, and critical infrastructure.

This “2023–2024 CISA Roadmap for Artificial Intelligence” serves as a guide for CISA’s AI-related efforts, ensuring both internal coherence as well as alignment with the whole-of-government AI strategy. This roadmap incorporates key CISA-led actions as directed by Executive Order 14110, along with additional actions CISA is leading to promote AI security and support critical infrastructure owners and operators as they navigate the adoption of AI.

The roadmap includes CISA’s efforts to:

- Promote beneficial uses of AI to enhance cybersecurity capabilities and other aspects of CISA’s mission;
- Protect the nation’s AI systems from cybersecurity threats; and
- Deter malicious actors’ use of AI capabilities to threaten critical infrastructure.

The security challenges associated with AI parallel cybersecurity challenges associated with previous generations of software that manufacturers did not build to be secure by design, putting the burden of security on the customer. Although AI software systems might differ from traditional forms of software, fundamental security practices still apply. Thus, CISA’s AI roadmap builds on the agency’s cybersecurity and risk management programs. Critically, manufacturers of AI systems must follow secure by design principles: taking ownership of security outcomes for customers, leading product development with radical transparency and accountability, and making secure by design a top business priority. As the use of AI grows and becomes increasingly incorporated into critical systems, security must be a core requirement and integral to AI system development from the outset and throughout its lifecycle.

VISION

We envision a future in which AI systems advance our nation's cyber defense, where our critical infrastructure is resilient and protected from malicious use of AI, and where AI developers prioritize the security of their products as a core business requirement.

CISA'S ROLE IN SECURING AI

CISA's Strategic Plan 2023–2025 underpins CISA's adaptation to these technologies and each of CISA's four strategic goals are relevant to and impacted by AI:

GOAL 1 | CYBER DEFENSE. AI tools can help defend cyberspace against traditional threats, as well as emerging AI-driven threats. However, AI-based software systems are also software systems that require securing and necessitate cyber defense for AI.

GOAL 2 | RISK REDUCTION AND RESILIENCE. Critical infrastructure organizations increasingly use AI systems to maintain and improve resilience. CISA will guide and support responsible and risk-aware adoption of AI-based software systems that are secure by design.

GOAL 3 | OPERATIONAL COLLABORATION. As AI contributes to a rapidly changing threat landscape, CISA will communicate threat and risk information to the U.S. public, including critical infrastructure sectors. Furthermore, AI companies and AI use cases may be subject to targeted threats and may require specific services and protections in response.

GOAL 4 | AGENCY UNIFICATION. CISA will responsibly integrate AI software systems across the agency, as well as recruit and develop a workforce capable of optimally harnessing AI software systems to carry out CISA's mission.

FIVE LINES OF EFFORT

This roadmap represents our work to unify and accelerate CISA's AI efforts along five lines of effort (LOE):

LINE OF EFFORT 1:

Responsibly use AI to support our mission. CISA will use AI-enabled software tools to strengthen cyber defense and support our critical infrastructure mission. CISA's adoption of AI will ensure responsible, ethical, and safe use—consistent with the Constitution and all applicable laws and policies, including those addressing federal procurement, privacy, civil rights, and civil liberties.

LINE OF EFFORT 2:

Assure AI systems. CISA will assess and assist secure by design, AI-based software adoption across a diverse array of stakeholders, including federal civilian government agencies; private sector companies; and state, local, tribal, and territorial (SLTT) governments through the development of best practices and guidance for secure and resilient AI software development and implementation.

LINE OF EFFORT 3:

Protect critical infrastructure from malicious use of AI. CISA will assess and recommend mitigation of AI threats facing our nation's critical infrastructure in partnership with other government agencies and industry partners that develop, test, and evaluate AI tools.

LINE OF EFFORT 4:

Collaborate with and communicate on key AI efforts with the interagency, international partners and the public. CISA will contribute to DHS-led and interagency processes on AI-enabled software. This LOE includes developing policy approaches for the U.S. government's overall national strategy on AI and supporting a whole-of-DHS approach on AI-based-software policy issues. This LOE also includes coordinating with international partners to advance global AI security best practices and principles.

LINE OF EFFORT 5:

Expand AI expertise in our workforce. CISA will continue to educate our workforce on AI software systems and techniques, and the agency will continue to actively recruit interns, fellows, and future employees with AI expertise. CISA will ensure that internal training reflects—and new recruits understand—the legal, ethical, and policy aspects of AI-based software systems in addition to the technical aspects.

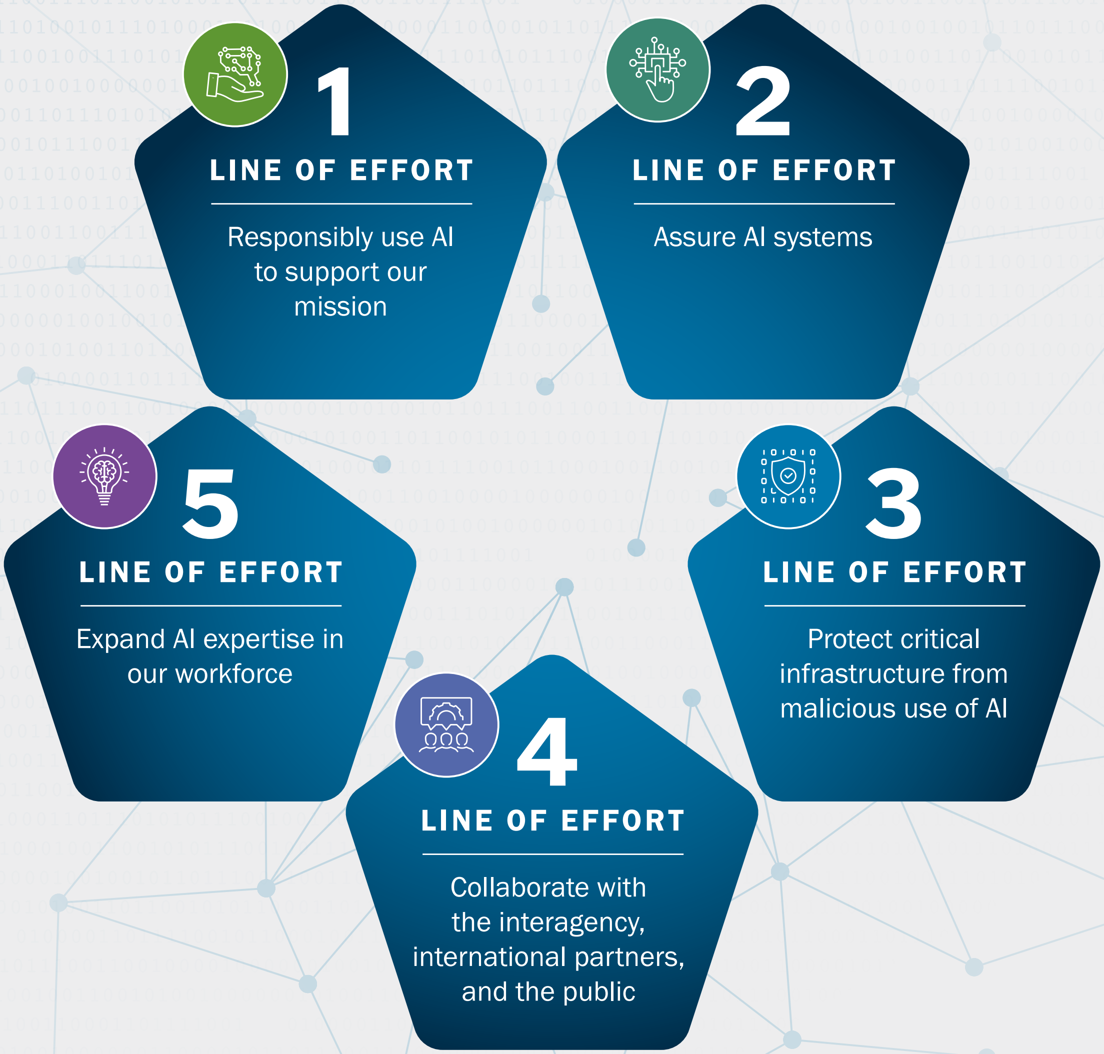

1
LINE OF EFFORT
Responsibly use AI to support our mission
2
LINE OF EFFORT
Assure AI systems
3
LINE OF EFFORT
Protect critical infrastructure from malicious use of AI
4
LINE OF EFFORT
Collaborate with the interagency, international partners, and the public
5
LINE OF EFFORT
Expand AI expertise in our workforce

Figure 1. CISA's roadmap for artificial intelligence lines of effort

This roadmap provides objectives for each line of effort that detail how CISA will accomplish these goals and measure our success. We also include representative outcomes and a notional measurement approach for each line of effort. We are developing more specific measures of effectiveness, which will be defined in our annual operating plans. Of note, identifying appropriate measures of effectiveness and vice measurements of performance is challenging and will require an ongoing effort—with continuous refinements as needed—throughout the life of the plan.

LINE OF EFFORT 1

RESPONSIBLY USE AI TO SUPPORT OUR MISSION

CISA will use AI-enabled software tools to strengthen cyber defense and support our critical infrastructure mission. CISA's adoption of AI will ensure responsible, ethical, and safe use—consistent with the Constitution and all applicable laws and policies, including those addressing federal procurement, privacy, civil rights, and civil liberties.

REPRESENTATIVE OUTCOMES

1 | CISA assesses our cybersecurity programs for potential uses of AI and provides the resources, requirements, and oversight to incorporate AI where appropriate.

2 | Through the responsible use of AI tools, CISA network defenders proactively mitigate threats to critical networks before damaging intrusions occur.

MEASUREMENT APPROACH

Increased responsible uses of AI software tools across CISA workflows.

OBJECTIVE 1.1 | Establish governance and oversight processes for CISA's use of AI.

CISA will establish robust AI governance processes to coordinate actions across the agency. This will include developing ethical and safety oversight processes as well as legal, procurement, privacy, civil rights, and civil liberties considerations. Responsible use will be central to our application of AI.

To promote responsible AI use, CISA will:

- Create our own NIST AI Risk Management Framework (RMF) profile to help develop and implement security and privacy controls for AI;
- Implement a programmatic structure for AI adoption within cyber defense missions;
- Review active AI use cases;
- Develop workplace guidance for generative technologies; and,
- Address AI data requirements and uses.

OBJECTIVE 1.2 | Collect, review, and prioritize AI use cases to support CISA missions.

CISA will create an agency AI Use Case Inventory to collect, review, and prioritize AI use cases supporting our missions. This inventory will encompass improvements to existing IT systems, collaboration tools, workflows, critical infrastructure defense programs, and proposed data collections for training AI models.

OBJECTIVE 1.3 | Develop an adoption strategy for the next generation of AI-enabled technologies.

To stay ahead of the adoption curve while ensuring privacy and civil rights protections, CISA will closely coordinate AI-related research and development efforts to target gaps in mission needs. These initiatives include the identification of baseline responsible practices for AI to protect safety and rights, the creation of a safe and secure AI testbed, and the development of technical requirements for cybersecurity use cases.

OBJECTIVE 1.4 | Incorporate cyber defense, incident management, and redress procedures into AI systems and processes.

CISA will establish incident response capabilities for AI usage, including remedy and redress procedures when necessary. In addition, CISA will adopt an approach for continuous evaluation of AI models while reviewing IT security practices to securely integrate AI technology.

OBJECTIVE 1.5 | Examine holistic approaches to limiting bias in AI use at CISA.

CISA will explore holistic approaches to limit bias in AI use, identifying potential bias points in the development, testing, implementation, and maintenance processes in order to build in fairness. Beyond exploring bias and mitigation strategies, CISA will develop a quality assessment for training data and public notice of our AI Use Case Inventory.

OBJECTIVE 1.6 | Responsibly and securely deploy AI systems to support CISA's cybersecurity mission.

Responsible and secure AI deployment aligns with CISA's core cybersecurity mission. To help ensure this, CISA will explore the identification, testing, evaluation, and deployment of AI capabilities for cyber defense, including detection of vulnerabilities in critical U.S. government software, systems, and networks, and we will document the lessons learned.

LINE OF EFFORT 2

ASSURE AI SYSTEMS

CISA will assess and assist secure by design AI-based software adoption across a diverse array of stakeholders, including federal civilian government agencies; private sector companies; and state, local, tribal, and territorial (SLTT) governments through the development of best practices and guidance for secure and resilient AI software development and implementation.

REPRESENTATIVE OUTCOMES

1 | CISA identifies cybersecurity risks and security resilience challenges as early as possible during AI adoption to mitigate threats to critical infrastructure.

2 | CISA adapts existing security guidance and service offerings to AI software systems, including best practices for red teaming AI systems and for making AI software that is secure by design.

3 | Stakeholders understand how AI-specific vulnerabilities fit into the existing coordinated vulnerability disclosure process.

MEASUREMENT APPROACH

Increased adherence to CISA risk guidance and best practices for AI software deployment, including guidance on red teaming and vulnerability mangement.

OBJECTIVE 2.1 | Assess cybersecurity risks of AI adoption in critical infrastructure sectors.

CISA will assess potential risks related to the use of AI in critical infrastructure sectors, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyberattacks. CISA will then consider ways to mitigate these vulnerabilities. Additionally, CISA will incorporate the NIST AI Risk Management Framework (AI RMF 1.0), as well as other appropriate security guidance, into relevant safety and security guidelines and best practices for use by critical infrastructure owners and operators.

OBJECTIVE 2.2 | Engage critical infrastructure stakeholders to determine security and resilience challenges of AI adoption.

CISA will engage with critical infrastructure stakeholders to assess and address the use of AI across critical infrastructure sectors.

OBJECTIVE 2.3 | Capture the breadth of AI systems used across the federal enterprise.

CISA will evaluate Software Bill of Materials (SBOM) toolchains, including SBOM format standards and automated SBOM collection and translation software, to confirm coverage of AI software.

OBJECTIVE 2.4 | Develop best practices and guidance for acquisition, development, and operation of secure AI systems.

CISA will develop best practices and guidance for the acquisition, development, and operation of secure AI systems. We will also provide guidance for the secure use of AI technologies and will integrate this guidance into the Cybersecurity Performance Goals pertaining to AI and related systems.

OBJECTIVE 2.5 | Drive adoption of strong vulnerability management practices for AI systems.

CISA will develop tools and techniques to harden and test AI systems, as well as incorporate appropriate outputs of adversarial ML processes and AI system vulnerabilities into the National Vulnerability Database. This includes conducting an operational test of an AI vulnerability in the Coordinated Vulnerability Disclosure (CVD) process, as well as writing strategic guidance for security testing and red teaming AI systems and software, particularly Open Source Software.

OBJECTIVE 2.6 | Incorporate AI systems into Secure by Design initiative.

CISA champions a secure by design approach to developing and manufacturing technology products, ensuring manufacturers design products with security in mind at the onset, so consumers receive products that are secure right out of the box. To encourage a secure by design approach to AI software and products, CISA will integrate AI security into the Secure by Design program and will develop a research pipeline to continually understand and project ways to support AI systems security.

LINE OF EFFORT 3

PROTECT CRITICAL INFRASTRUCTURE FROM MALICIOUS USE OF AI

CISA will assess and recommend mitigation of AI threats against our nation's critical infrastructure in partnership with other government agencies and industry partners that develop, test, and evaluate AI tools.

REPRESENTATIVE OUTCOMES

1 | Through engagement with stakeholders, including tabletop exercises focused on AI-enhanced attacks, CISA protects AI systems from adversarial manipulation or abuse.

2 | CISA supports the advancement of AI risk management practices across the critical infrastructure community through the publication and dissemination of decision support materials, such as a risk management guide for AI risks to critical infrastructure.

MEASUREMENT APPROACH:

Number of publications and engagements that support shared awareness of emerging AI-related risks and advances in AI risk management practices.

OBJECTIVE 3.1 | Regularly engage industry stakeholder partners that are developing AI tools to assess and address security concerns to critical infrastructure and evaluate methods for educating partners and stakeholders.

CISA will build on existing structures to advance industry collaboration and coordination around AI security. The Information Technology Sector Coordinating Council's AI Working Group, which was established in March 2023, will continue to provide advice on AI security challenges and feedback on agency AI initiatives.

CISA will also stand up an operational effort in the Joint Cyber Defense Collaborative (JCDC), JCDC.AI, to catalyze focused collaboration around threats, vulnerabilities, and mitigations affecting AI systems. The JCDC effort will also explore potential operational planning efforts that bring together AI providers and critical infrastructure operators to address specific risks.

OBJECTIVE 3.2 | Use CISA partnerships and working groups to share information on AI-driven threats.

CISA will use agency partnerships and working groups, including JCDC.AI, to share information on AI-driven threats. The agency will engage industry, federal, and international partners to understand emerging threats and share them with the broader commuity.

OBJECTIVE 3.3 | Assess AI risks to critical infrastructure.

Each critical infrastructure sector has a unique set of needs and capabilities. As adversaries adopt AI-enabled software systems and as AI expands the cyber threat landscape, CISA will publish materials to raise awareness of emerging risks. CISA will also evaluate risk management approaches and methodologies to determine the appropriate analytical framework for the assessment and treatment of AI risks and will identify necessary enhancements.

LINE OF EFFORT 4

COLLABORATE WITH AND COMMUNICATE ON KEY AI EFFORTS WITH THE INTERAGENCY, INTERNATIONAL PARTNERS, AND THE PUBLIC

CISA will contribute to DHS-led and interagency processes on AI-enabled software. This LOE includes developing policy approaches for the U.S. government's overall national strategy on AI and supporting a whole-of-DHS approach on AI-based-software policy issues. This LOE also includes coordinating with international partners to advance global AI best practices and principles.

REPRESENTATIVE OUTCOMES

1 | CISA stakeholders are aligned around clear guidance for AI security.

MEASUREMENT APPROACH

Proportion of AI-focused guidance and policy documents developed in collaboration with U.S. interagency and international partners.

OBJECTIVE 4.1 | Support the development of a whole-of-DHS approach on AI policy issues.

CISA will support the development of a whole-of-DHS approach to AI policy issues. As CISA develops our agency-specific AI efforts, we will closely coordinate with DHS entities, including the DHS AI Task Force.

OBJECTIVE 4.2 | Participate in interagency policy meetings and interagency working groups on AI.

CISA will attend interagency meetings to foster coherent and collaborative approaches to federal government AI policy.

OBJECTIVE 4.3 | Develop CISA policy positions that take a strategic, national level perspective for AI policy documents, such as memoranda and other products.

CISA will develop policy positions that take a strategic, national level perspective for AI policy documents and ensure alignment of CISA strategies, priorities, and policies with interagency doctrine. CISA will drive policy decisions to support critical infrastructure equities and integrate national strategic level perspectives in key AI policy documents. Additionally, to increase public awareness about AI assurance, CISA will develop AI assurance publications.

OBJECTIVE 4.4 | Ensure CISA strategy, priorities, and policy framework align with interagency policies and strategy.

CISA will work across the interagency to ensure CISA policies and strategies align with the whole-of-government approach to AI.

OBJECTIVE 4.5 | Engage with international partners surrounding global AI security.

CISA will co-develop and co-seal guidance for AI security with other federal agencies and international partners. CISA will engage with international partners surrounding global AI security and encourage the adoption of international best practices for secure AI.

LINE OF EFFORT 5

EXPAND AI EXPERTISE IN OUR WORKFORCE

CISA will continue to educate our workforce on AI software systems and techniques, and the agency will continue to actively recruit interns, fellows, and future employees with AI expertise. CISA will ensure that internal training reflects—and new recruits understand—the legal, ethical, and policy aspects of AI-based software systems in addition to the technical aspects.

REPRESENTATIVE OUTCOMES

1 | CISA hires, trains, and retains a workforce with AI expertise.

MEASUREMENT APPROACH

Increased AI expertise in the CISA workforce.

OBJECTIVE 5.1 | Connect and amplify AI expertise that already exists in CISA's workforce.

As the nation's cyber defense agency, the CISA team includes a strong workforce of cybersecurity experts. The agency will identify and leverage existing AI expertise across CISA. We will also develop an AI community of practice for engagement across the agency, as well as maintain key points of contact from each division leading AI activities, positioning the agency for a collaborative and cohesive approach to expanding our AI capabilities.

OBJECTIVE 5.2 | Recruit interns, fellows, and staff with AI expertise.

CISA will recruit interns, fellows, and staff with AI expertise. CISA will use a variety of pathways, including the Cyber Talent Management System (CTMS), for recruiting, developing, and maintaining our AI workforce.

OBJECTIVE 5.3 | Educate CISA's workforce on AI.

CISA will provide training and education opportunities for employees on an ongoing basis as part of our plan to help our workforce have the knowledge and skills to engage, innovate, and apply appropriately the current and emerging capabilities afforded by AI.

OBJECTIVE 5.4 | Ensure internal training not only reflects technical expertise, but also incorporates legal, ethical, and policy considerations of AI implementation across all aspects of CISA's work.

CISA will provide access to training that includes objectives on legal, ethical, and policy aspects of implementing AI.

CONCLUSION

A whole-of-government approach is needed to fully harness the benefits and mitigate the risks of AI. Through the initiatives outlined in this roadmap, CISA strives toward our vision of a nation in which AI systems advance our nation's cyber defense, where our critical infrastructure is resilient and protected from malicious use of AI, and where AI developers prioritize the security of their products as a core business requirement.

KEY DEFINITIONS

ARTIFICIAL INTELLIGENCE (AI)

Within this document, "Artificial intelligence" (AI) has the meaning[1] set forth in the *National Artificial Intelligence Initiative Act of 2020* (enacted as Division E of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Section 5002(3):

A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to:

> **(A)** perceive real and virtual environments;
> **(B)** abstract such perceptions into models through analysis in an automated manner; and,
> **(C)** use model inference to formulate options for information or action.

AI encompasses machine learning (ML), which, according to Executive Order 14110 is "a set of techniques that can be used to train AI algorithms to improve performance on a task based on data."

AI ASSURANCE

Many terms are shared between the AI and information security communities, but the same term can carry different and incompatible meanings. Because this roadmap is relevant to both communities, this document incorporates both sets of meanings. As an example, both communities have developed special uses of "assurance" independently since at least the 1980s:

AI ASSURANCE: "A process that is applied at all stages of the AI engineering lifecycle ensuring that any intelligent system is producing outcomes that are valid, verified, data-driven, trustworthy and explainable to a layman, ethical in the context of its deployment, unbiased in its learning, and fair to its users."[2]

SECURITY ASSURANCE: "Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the security policy."[3]

When this document simply says "assurance" or uses another shared term without distinguishing the origin, this document incorporates **both** communities' meanings.

[1] There are other statutory definitions for artificial intelligence. The "AI in Government Act of 2020" (P.L. 116-260, Division U, Title I, codified at 40 U.S.C. § 11301, note), listed earlier in this document, uses the definition from § 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, (P.L. 116-232, codified at 10 U.S.C. § 2358 note).
The term ''artificial intelligence'' includes the following:
(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
(3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.
(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

[2] Batarseh FA, Freeman L, Huang CH. A survey on artificial intelligence assurance. Journal of Big Data. 2021 Apr 26;8(1):60. A survey on artificial intelligence assurance | Journal of Big Data (springer.com)

AI SECURITY

AI Security is a term encompassing several different categories of cybersecurity, including the three key categories addressed in this roadmap:

1. Applications of AI for cybersecurity: CISA actively leverages AI tools for threat detection, prevention, and vulnerability assessments.

2. Cybersecurity of AI-enabled systems: CISA is applying traditional cybersecurity principles and practices to protect and secure AI-enabled systems. In addition to being well-positioned to leverage our existing expertise, CISA is advancing AI-enabled systems security through efforts to promote secure by design best practices for AI-enabled software systems.

3. Threats from Adversarial Use of AI: CISA, in collaboration with other parts of DHS, will focus on research, development, and acquisition of tools to improve the resilience of federal civilian executive branch (FCEB) agencies and critical infrastructure and to protect these agencies and organizations from malicious uses of AI.

RED TEAMING

As defined in Executive Order 14110, AI red teaming is "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI systems. AI red-teaming is most often performed by dedicated 'red teams' that adopt adversarial methods to identify flaws, vulnerabilities, or logic errors, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system."

The goals of security testing and red teaming (whether on AI systems or not) are to identify vulnerabilities in a system and better manage the associated security posture. During a cybersecurity red team assessment, a red team attempts to gain access to an organization's enterprise network and trigger a security response from the organization's people, processes, or technology.

ADVERSARIAL MACHINE LEARNING

Malicious cyber actors target vulnerabilities throughout the AI supply chain to cause certain behavior, unintended by the system owner or operator, in machine learning (ML) systems—referred to as adversarial machine learning. For example, malicious actors may manipulate training data, affect the performance of the ML model's classification and regression, or exfiltrate sensitive ML model information. For more information on adversarial machine learning, including information on types of activity, see National Institute of Standards and Technology (NIST), Technical Series Publication Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations and MITRE ATLAS Adversarial Machine Learning 101.

[3] NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View. This definition is also very similar to the international IETF definition in RFC 4949.

[4] CISA Cybersecurity Advisory: CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks

[5] Poison Training Data. MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems) Techniques. https://atlas.mitre.org/techniques/AML.T0020/.

APPENDIX

RECENT U.S. EFFORTS ON AI POLICY

Recent actions taken by the U.S. government's executive and legislative branches related to AI-based software systems reflect the need to marshal a national effort to defend critical infrastructure and government networks and assets, work with partners across government and industry, and expand existing services and programs for federal civilian agencies and critical infrastructure owners and operators. The following recent efforts guide CISA's actions in this plan:

Executive Order 14110 "Safe, Secure, And Trustworthy Development and Use of Artificial Intelligence (AI)." (October 2023) This EO focuses on ensuring that AI is safe and secure. This will require robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and mechanisms to test, understand, and mitigate risks from these systems before they are put to use.

Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI. (Updated September 2023) The Biden-Harris administration has secured voluntary commitments from leading AI companies to help move toward safe, secure, and transparent development of the AI technology. These commitments include ensuring products are safe before introducing them to the public, building systems that put security first, and earning the public's trust.

DHS Policy Statement 139-06 Acquisition and Use of Artificial Intelligence and Machine Learning by DHS Components. (August 2023) This policy statement provides that DHS will acquire and use AI only in a manner that is consistent with the Constitution and all other applicable laws and policies.

New National Science Foundation Funding. (May 2023) This dedicated $140 million will launch seven new National AI Research Institutes to promote responsible innovation, bolster America's AI research and development (R&D) infrastructure and support the development of a diverse AI workforce.

AI Risk Management Framework (RMF). (January 2023) In collaboration with the private and public sectors, the National Institute of Standards and Technology (NIST) developed this framework to better manage risks—to individuals, organizations, and society—that are uniquely associated with AI. The NIST AI RMF, intended for voluntary use, aims to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.

Blueprint for an AI Bill of Rights. **(October 2022)** This framework is a set of five principles—identified by the White House Office of Science and Technology Policy—that should guide the design, use, and deployment of automated systems to protect the American public in the age of AI.

2021 Final Report of the National Security Commission on Artificial Intelligence. **(March 2021)** This report presented an integrated national strategy to reorganize the government, reorient the nation, and rally our closest allies and partners to defend and compete in the coming era of AI-accelerated competition and conflict.

National Artificial Intelligence Initiative (NAII) Act of 2020 (Division E of the National Defense Authorization Act for Fiscal Year 2021). **(January 2021)** Among other things, this act established direction and authority to coordinate AI research, development, and demonstration activities among civilian agencies, the Department of Defense, and the intelligence community to ensure that each informs the work of the others.

AI in Government Act of 2020 (Title I of Division U of the Consolidated Appropriations Act, 2021). **(December 2020)** This act created the AI Center of Excellence within the General Services Administration and directed the Office of Management and Budget (OMB) to issue a memorandum informing federal agencies of policies for acquisition and application of AI and identifying best practices for mitigating risks.

Department of Homeland Security 2020 Artificial Intelligence Strategy. **(December 2020)** This strategy set out to enhance DHS's capability to safeguard the American people, our homeland, and our values through the responsible integration of AI into DHS's activities and the mitigation of new risks posed by AI.

EO 13960: Promoting the Use of Trustworthy AI in the Federal Government. **(December 2020)** This executive order required federal agencies to inventory their AI use cases and share their inventories with other government agencies and the public.

EO 13859: Maintaining American Leadership in AI. **(February 2019)** This executive order established federal principles and strategies to strengthen the nation's capabilities in AI to promote scientific discovery, economic competitiveness, and national security.

2023–2024

CISA ROADMAP FOR ARTIFICIAL INTELLIGENCE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

23andMe tells victims it's their fault that their data was breached

Lorenzo Franceschi-Bicchierai

@lorenzofb / 11:42 AM EST • January 3, 2024

Comment

Image Credits: Gabe Ginsberg/Getty Images for LARAS

Facing more than 30 lawsuits from victims of its massive data breach, 23andMe is now deflecting the blame to the victims themselves in an attempt to absolve itself from any responsibility, according to a letter sent to a group of victims seen by TechCrunch.

"Rather than acknowledge its role in this data security disaster, 23andMe has apparently decided to leave its customers out to dry while downplaying the seriousness of these events," Hassan Zavareei, one of the lawyers representing the victims who received the letter from 23andMe, told TechCrunch in an email.

In December, 23andMe admitted that hackers had stolen the genetic and ancestry data of 6.9 million users, nearly half of all its customers.

The data breach started with hackers accessing only around 14,000 user accounts. The hackers broke into this first set of victims by brute-forcing accounts with passwords that were known to be associated with the targeted customers, a technique known as credential stuffing.

From these 14,000 initial victims, however, the hackers were able to then access the personal data of the other 6.9 million victims because they had opted-in to 23andMe's DNA Relatives feature. This optional feature allows customers to automatically share some of their data with people who are considered their relatives on the platform.

In other words, by hacking into only 14,000 customers' accounts, the hackers subsequently scraped personal data of another 6.9 million customers whose accounts were not directly hacked.

But in a letter sent to a group of hundreds of 23andMe users who are now suing the company, 23andMe said that “users negligently recycled and failed to update their passwords following these past security incidents, which are unrelated to 23andMe.”

“Therefore, the incident was not a result of 23andMe’s alleged failure to maintain reasonable security measures,” the letter reads.

Zavareei said that 23andMe is “shamelessly” blaming the victims of the data breach.

“This finger pointing is nonsensical. 23andMe knew or should have known that many consumers use recycled passwords and thus that 23andMe should have implemented some of the many safeguards available to protect against credential stuffing — especially considering that 23andMe stores personal identifying information, health information, and genetic information on its platform,” Zavareei said in an email.

“The breach impacted millions of consumers whose data was exposed through the DNA Relatives feature on 23andMe’s platform, not because they used recycled passwords. Of those millions, only a few thousand accounts were compromised due to credential stuffing. 23andMe’s attempt to shirk responsibility by blaming its customers

Login

Search

Startups
Venture
Security
AI
Crypto
Apps
Events
Startup Battlefield
More

does nothing for these millions of consumers whose data was compromised through no fault of their own whatsoever," said Zavareei.

CONTACT US

Do you have more information about the 23andMe incident? We'd love to hear from you. You can contact Lorenzo Franceschi-Bicchierai securely on Signal at +1 917 257 1382, or via Telegram, Keybase and Wire @lorenzofb, or email lorenzo@techcrunch.com. You also can contact TechCrunch via SecureDrop.

In response to 23andMe's letter, Dante Termohs, a 23andMe customer who was impacted by the data breach, told TechCrunch that he found "it appalling that 23andMe is attempting to hide from consequences instead of helping its customers."

23andMe's lawyers argued that the stolen data cannot be used to inflict monetary damage against the victims.

"The information that was potentially accessed cannot be used for any harm. As explained in the October 6, 2023 blog post, the profile information that may have been accessed related to the DNA Relatives feature, which a customer creates and chooses to share with other users on 23andMe's platform. Such information would only be available if plaintiffs affirmatively elected to share this information with other users via the DNA Relatives feature. Additionally, the information that the unauthorized actor potentially obtained about plaintiffs could not have been used to cause pecuniary harm (it did not include their social security number, driver's license number, or any payment or financial information)," the letter read.

23andMe and one of its lawyers did not respond to TechCrunch's request for comment.

After disclosing the breach, 23andMe reset all customer passwords, and then required all customers to use multi-factor authentication, which was only optional before the breach.

In an attempt to pre-empt the inevitable class action lawsuits and mass arbitration claims, 23andMe changed its terms of service to make it more difficult for victims to band together when filing a legal claim against the company. Lawyers with experience representing data breach victims told TechCrunch that the changes were "cynical," "self-serving" and "a desperate attempt" to protect itself and deter customers from going after the company.

Clearly, the changes didn't stop what is now a flurry of class action lawsuits.

23andMe confirms hackers stole ancestry data on 6.9 million users

On Friday, genetic testing company 23andMe announced that hackers accessed the personal data of 0.1% of customers, or about 14,000 individuals. The company also said that by accessing those accounts, hackers were also able to access “a significant number of files

Login

Search

Startups
Venture
Security
AI
Crypto
Apps
Events
Startup Battlefield
More

Login

Search

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup Battlefield

More

https://tcrn.ch/48qpcXG Copy

Tags

23andMe class action cybersecurity

data breach Exclusive hackers

hacking

OpenAI announces new board members, reinstates CEO Sam Altman

Kyle Wiggers

5:58 PM EST • March 8, 2024

Techstars' $80M partnership with J.P. Morgan is on the rocks, employees say

Dominic-Madori Davis

5:30 PM EST • March 8, 2024

Bumble lost a third of its Texas workforce after state passed restrictive 'Heartbeat Act' abortion bill

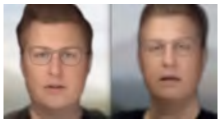
Sarah Perez

5:12 PM EST • March 8, 2024

Two former CloudKitchens execs are tackling Mexico's solar power lag

Tim De Chant

4:43 PM EST • March 8, 2024



Hey, it's me, Brian's less creepy Apple Vision Pro Persona

Brian Heater

3:08 PM EST • March 8, 2024

The incumbents go shopping for startups

Haje Jan Kamps

3:05 PM EST • March 8, 2024

Rivian's new 'treehouse' rooftop tent comes with a movie projector

Kirsten Korosec

3:02 PM EST • March 8, 2024

Only 7 days left to save $1,000 on Disrupt passes

Robert Frawley

3:00 PM EST • March 8, 2024

Women in AI: Sarah Kreps, professor of government at Cornell

Kyle Wiggers

2:57 PM EST • March 8, 2024

The women in AI making a difference

Kyle Wiggers, Dominic-Madori Davis

2:57 PM EST • March 8, 2024

How DMA gatekeepers are responding to the EU's new competition rules — in their own words

Natasha Lomas

2:11 PM EST • March 8, 2024

Fortnite is coming back to iOS in Europe (for real this time)

Amanda Silberling

1:49 PM EST • March 8, 2024

Despite distancing itself from politics, the topic is dominating Threads' trends

Sarah Perez

12:32 PM EST • March 8, 2024

Pitch Deck Teardown: Astek Diagnostics's $2M seed deck

Haje Jan Kamps

12:00 PM EST • March 8, 2024

GM resumes Chevy Blazer EV sales with new software and lower prices

Kirsten Korosec

12:00 PM EST • March 8, 2024

Reddit launches free tools to help businesses grow their presence on the site ahead of IPO

Aisha Malik

11:04 AM EST • March 8, 2024

Profitable car rental service Turo is still ready for an IPO, but its growth cratered in 2023

Alex Wilhelm

11:01 AM EST • March 8, 2024

Creator wishlist startup Throne is doing so well that it returned investor money

Ivan Mehta

11:00 AM EST • March 8, 2024

The Rivian R2 SUV racks up 68,000 reservations a day after reveal

Kirsten Korosec

10:53 AM EST • March 8, 2024

Spyware makers express concern after US sanctions spyware veteran

Lorenzo Franceschi-Bicchierai

10:48 AM EST • March 8, 2024

Login

Search

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup Battlefield

More

About

TechCrunch

Staff

Contact Us

Advertise

Crunchboard Jobs

Site Map

Legal

Terms of Service

Privacy Policy

RSS Terms of Use

Privacy Dashboard

Code of Conduct

About Our Ads

Trending Tech Topics

Anthropic Claude 3 Chatbot

Apple M3 MacBook Air Review

Spotify Price Increase

Crypto Perfume

Rivian R3 Hatchback

Tech Layoffs

ChatGPT

Login

Search

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup Battlefield

More

ALERT

CISA Adds One Known Exploited Vulnerability to Catalog

Release Date: September 19, 2023

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>, based on evidence of active exploitation.

- CVE-2023-28434 <https://nvd.nist.gov/vuln/detail/cve-2023-28434> MinIO Security Feature Bypass Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. **Note:** To view other newly added vulnerabilities in the catalog, click on the arrow in the "Date Added to Catalog" column—which will sort by descending dates.

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities <https://www.cisa.gov/binding-operational-directive-22-01> established the Known Exploited Vulnerabilities Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet <https://www.cisa.gov/sites/default/files/publications/reducing_the_significant_risk_of_known_exploited_vulnerabilities_211103.pdf> for more information.

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria <https://www.cisa.gov/known-exploited-vulnerabilities>.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we’d welcome your feedback.

Related Advisories

MAR 08, 2024 **ALERT**

Apple Released Security Updates for Multiple Products </news-events/alerts/2024/03/08/apple-released-security-updates-multiple-products>

MAR 07, 2024 **ALERT**

CISA Releases One Industrial Control Systems Advisory </news-events/alerts/2024/03/07/cisa-releases-one-industrial-control-systems-advisory>

MAR 07, 2024 **ALERT**

Apple Releases Security Updates for iOS and iPadOS </news-events/alerts/2024/03/07/apple-releases-security-updates-ios-and-ipados>

MAR 07, 2024 **ALERT**

CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices </news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

888-282-0870 central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility </accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so. The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society.

In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. I firmly believe that the power of our ideals; the foundations of our society; and the creativity, diversity, and decency of our people are the reasons that America thrived in past eras of rapid change. They are the reasons we will succeed again in this moment. We are more than capable of harnessing AI for justice, security, and opportunity for all.

Sec. 2. Policy and Principles. It is the policy of my Administration to advance and govern the development and use of AI in accordance with eight guiding principles and priorities. When undertaking the actions set forth in this order, executive departments and agencies (agencies) shall, as appropriate and consistent with applicable law, adhere to these principles, while, as feasible, taking into account the views of other agencies, industry, members of academia, civil society, labor unions, international allies and partners, and other relevant organizations:

(a) Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers — while navigating AI's opacity and complexity. Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies. Finally, my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits.

(b) Promoting responsible innovation, competition, and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges. This effort requires investments in AI-related education, training, development, research, and capacity, while simultaneously tackling novel intellectual property (IP) questions and other problems to protect inventors and creators. Across the Federal Government, my Administration will support programs to provide Americans the skills they need for the age of AI and attract the world's AI talent to our shores — not just to study, but to stay — so that the companies and technologies of the future are made in America. The Federal Government will promote a fair, open, and competitive ecosystem and marketplace for AI and related technologies so that small developers and entrepreneurs can continue to drive innovation. Doing so requires stopping unlawful collusion and addressing risks from dominant firms' use of key assets such as semiconductors, computing power, cloud storage, and data to disadvantage competitors, and it requires supporting a marketplace that harnesses the benefits of AI to provide new opportunities for small businesses, workers, and entrepreneurs.

(c) The responsible development and use of AI require a commitment to supporting American workers. As AI creates new jobs and industries, all workers need a seat at the table, including through collective bargaining, to ensure that they benefit from these opportunities. My Administration will seek to adapt job training and education to support a diverse workforce and help provide access to opportunities that AI creates. In the workplace itself, AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions. The critical next steps in AI development should be built on the views of workers, labor unions, educators, and employers to support responsible uses of AI that improve workers' lives, positively augment human work, and help all people safely enjoy the gains and opportunities from technological innovation.

(d) Artificial Intelligence policies must be consistent with my Administration's dedication to advancing equity and civil rights. My Administration cannot — and will not — tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice. From hiring to housing to healthcare, we have seen what happens when AI use deepens discrimination and bias, rather than improving quality of life. Artificial Intelligence systems deployed irresponsibly have reproduced and intensified existing inequities, caused new types of harmful discrimination, and exacerbated online and physical harms. My Administration will build on the important steps that have already been taken — such as issuing the Blueprint for an AI Bill of Rights, the AI Risk Management Framework, and Executive Order 14091 of February 16, 2023 (Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government) — in seeking to ensure that AI complies with all Federal laws and to promote robust technical evaluations, careful oversight, engagement with affected communities, and rigorous regulation. It is necessary to hold those developing and deploying AI accountable to standards that protect against unlawful discrimination and abuse, including in the justice system and the Federal Government. Only then can Americans trust AI to advance civil rights, civil liberties, equity, and justice for all.

(e) The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected. Use of new technologies, such as AI, does not excuse organizations from their legal obligations, and hard-won consumer protections are more important than ever in moments of technological change. The Federal Government will enforce existing consumer protection laws and principles and enact appropriate safeguards against fraud, unintended bias, discrimination, infringements on privacy, and other harms from AI. Such protections are especially important in critical fields like healthcare, financial services, education, housing, law, and transportation, where mistakes by or misuse of AI could harm patients, cost consumers or small businesses, or jeopardize safety or rights. At the same time, my Administration will promote responsible uses of AI that protect consumers, raise the quality of goods and services, lower their prices, or expand selection and availability.

(f) Americans' privacy and civil liberties must be protected as AI continues advancing. Artificial Intelligence is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires. Artificial Intelligence's capabilities in these areas can increase the risk that personal data could be exploited and exposed. To combat this risk, the Federal Government will ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks. Agencies shall use available policy and technical tools, including privacy-enhancing technologies (PETs) where appropriate, to protect privacy and to combat the broader legal and societal risks — including the chilling of First Amendment rights — that result from the improper collection and use of people's data.

(g) It is important to manage the risks from the Federal Government's own use of AI and increase its internal capacity to regulate, govern, and support responsible use of AI to deliver better results for Americans. These efforts start with people, our Nation's greatest asset. My Administration will take steps to attract, retain, and develop public service-oriented AI professionals, including from underserved communities, across disciplines — including technology, policy, managerial, procurement, regulatory, ethical, governance, and legal fields — and ease AI professionals' path into the Federal Government to help harness and govern AI. The Federal Government will work to ensure that all members of its workforce receive adequate training to understand the benefits, risks, and limitations of AI for their job functions, and to modernize Federal Government information technology infrastructure, remove bureaucratic obstacles, and ensure that safe and rights-respecting AI is adopted, deployed, and used.

(h) The Federal Government should lead the way to global societal, economic, and technological progress, as the United States has in previous eras of disruptive innovation and change. This leadership is not measured solely by the technological advancements our country makes. Effective leadership also means pioneering those systems and safeguards needed to deploy technology responsibly — and building and promoting those safeguards with the rest of the world. My Administration will engage with international allies and partners in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges. The Federal Government will seek to promote responsible AI safety and security principles and actions with other nations, including our competitors, while leading key global conversations and collaborations to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms.

Sec. 3. Definitions. For purposes of this order:

(a) The term "agency" means each agency described in 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).

(b) The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

(c) The term "AI model" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

(d) The term "AI red-teaming" means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated "red teams" that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

(e) The term "AI system" means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

(f) The term "commercially available information" means any information or data about an individual or group of individuals, including an individual's or group of individuals' device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities.

(g) The term "crime forecasting" means the use of analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated without machines and based on statistics, such as historical crime statistics.

(h) The term "critical and emerging technologies" means those technologies listed in the February 2022 Critical and Emerging Technologies List Update issued by the National Science and Technology Council (NSTC), as amended by subsequent updates to the list issued by the NSTC.

(i) The term "critical infrastructure" has the meaning set forth in section 1016(e) of the USA PATRIOT Act of 2001, 42 U.S.C. 5195c(e).

(j) The term “differential-privacy guarantee” means protections that allow information about a group to be shared while provably limiting the improper access, use, or disclosure of personal information about particular entities.

(k) The term “dual-use foundation model” means an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by:

(i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or

(iii) permitting the evasion of human control or oversight through means of deception or obfuscation.

Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities.

(l) The term “Federal law enforcement agency” has the meaning set forth in section 21(a) of Executive Order 14074 of May 25, 2022 (Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety).

(m) The term “floating-point operation” means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base.

(n) The term “foreign person” has the meaning set forth in section 5(c) of Executive Order 13984 of January 19, 2021 (Taking Additional Steps To

Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities).

(o) The terms “foreign reseller” and “foreign reseller of United States Infrastructure as a Service Products” mean a foreign person who has established an Infrastructure as a Service Account to provide Infrastructure as a Service Products subsequently, in whole or in part, to a third party.

(p) The term “generative AI” means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

(q) The terms “Infrastructure as a Service Product,” “United States Infrastructure as a Service Product,” “United States Infrastructure as a Service Provider,” and “Infrastructure as a Service Account” each have the respective meanings given to those terms in section 5 of Executive Order 13984.

(r) The term “integer operation” means any mathematical operation or assignment involving only integers, or whole numbers expressed without a decimal point.

(s) The term “Intelligence Community” has the meaning given to that term in section 3.5(h) of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended.

(t) The term “machine learning” means a set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

(u) The term “model weight” means a numerical parameter within an AI model that helps determine the model’s outputs in response to inputs.

(v) The term “national security system” has the meaning set forth in 44 U.S.C. 3552(b)(6).

(w) The term “omics” means biomolecules, including nucleic acids, proteins, and metabolites, that make up a cell or cellular system.

(x) The term “Open RAN” means the Open Radio Access Network approach to telecommunications-network standardization adopted by the O-RAN Alliance, Third Generation Partnership Project, or any similar set of published open standards for multi-vendor network equipment interoperability.

(y) The term “personally identifiable information” has the meaning set forth in Office of Management and Budget (OMB) Circular No. A-130.

(z) The term “privacy-enhancing technology” means any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality. These technological means may include secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic-data-generation tools. This is also sometimes referred to as “privacy-preserving technology.”

(aa) The term “privacy impact assessment” has the meaning set forth in OMB Circular No. A-130.

(bb) The term “Sector Risk Management Agency” has the meaning set forth in 6 U.S.C. 650(23).

(cc) The term “self-healing network” means a telecommunications network that automatically diagnoses and addresses network issues to permit self-restoration.

(dd) The term “synthetic biology” means a field of science that involves redesigning organisms, or the biomolecules of organisms, at the genetic level to give them new characteristics. Synthetic nucleic acids are a type of biomolecule redesigned through synthetic-biology methods.

(ee) The term “synthetic content” means information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI.

(ff) The term “testbed” means a facility or mechanism equipped for conducting rigorous, transparent, and replicable testing of tools and technologies, including AI and PETs, to help evaluate the functionality, usability, and performance of those tools or technologies.

(gg) The term “watermarking” means the act of embedding information, which is typically difficult to remove, into outputs created by AI — including into outputs such as photos, videos, audio clips, or text — for the purposes of verifying the authenticity of the output or the identity or characteristics of its provenance, modifications, or conveyance.

Sec. 4. Ensuring the Safety and Security of AI Technology.

4.1. Developing Guidelines, Standards, and Best Practices for AI Safety and Security. (a) Within 270 days of the date of this order, to help ensure the development of safe, secure, and trustworthy AI systems, the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), in coordination with the Secretary of Energy, the Secretary of Homeland Security, and the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall:

(i) Establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, including:

(A) developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI;

(B) developing a companion resource to the Secure Software Development Framework to incorporate secure development practices for generative AI and for dual-use foundation models; and

(C) launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity.

(ii) Establish appropriate guidelines (except for AI used as a component of a national security system), including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems. These efforts shall include:

(A) coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models; and

(B) in coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies, as well as to support the design, development, and deployment of associated PETs, consistent with section 9(b) of this order.

(b) Within 270 days of the date of this order, to understand and mitigate AI security risks, the Secretary of Energy, in coordination with the heads of other Sector Risk Management Agencies (SRMAs) as the Secretary of Energy may deem appropriate, shall develop and, to the extent permitted by law and available appropriations, implement a plan for developing the Department of Energy's AI model evaluation tools and AI testbeds. The Secretary shall undertake this work using existing solutions where possible, and shall develop these tools and AI testbeds to be capable of assessing near-term extrapolations of AI systems' capabilities. At a minimum, the Secretary shall develop tools to evaluate AI capabilities to generate outputs that may represent nuclear, nonproliferation, biological, chemical, critical infrastructure, and energy-security threats or hazards. The Secretary shall do this work solely for the purposes of guarding against these threats, and shall also develop model guardrails that reduce such risks. The Secretary shall, as appropriate, consult with private AI laboratories, academia, civil society, and third-party evaluators, and shall use existing solutions.

4.2. Ensuring Safe and Reliable AI. (a) Within 90 days of the date of this order, to ensure and verify the continuous availability of safe, reliable, and effective AI in accordance with the Defense Production Act, as amended, 50 U.S.C. 4501 *et seq*., including for the national defense and the protection of critical infrastructure, the Secretary of Commerce shall require:

(i) Companies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records regarding the following:

(A) any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats;

(B) the ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights; and

(C) the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST pursuant to subsection 4.1(a)(ii) of this section, and a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security. Prior to the development of guidance on red-team testing standards by NIST pursuant to subsection 4.1(a)(ii) of this section, this description shall include the results of any red-team testing that the company has conducted relating to lowering the barrier to entry for the development, acquisition, and use of biological weapons by non-state actors; the discovery of software vulnerabilities and development of associated exploits; the use of software or tools to influence real or virtual events; the possibility for self-replication or propagation; and associated measures to meet safety objectives; and

(ii) Companies, individuals, or other organizations or entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster.

(b) The Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence, shall define, and thereafter update as needed on a regular basis, the set of technical conditions for models and computing clusters that would be subject to the reporting requirements of subsection 4.2(a) of this section. Until such technical conditions are defined, the Secretary shall require compliance with these reporting requirements for:

(i) any model that was trained using a quantity of computing power greater than 10^{26} integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10^{23} integer or floating-point operations; and

(ii) any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 10^{20} integer or floating-point operations per second for training AI.

(c) Because I find that additional steps must be taken to deal with the national emergency related to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended by Executive Order 13757 of December 28, 2016 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), and further amended by Executive Order 13984, to address the use of United States Infrastructure as a Service (IaaS) Products by foreign malicious cyber actors, including to impose additional record-keeping obligations with respect to foreign transactions and to assist in the investigation of transactions involving foreign malicious cyber actors, I hereby direct the Secretary of Commerce, within 90 days of the date of this order, to:

(i) Propose regulations that require United States IaaS Providers to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (a “training run”). Such reports shall include, at a minimum, the identity of the foreign person and the existence of any training run of an AI model meeting the criteria set forth in this section, or other criteria defined by the Secretary in regulations, as well as any additional information identified by the Secretary.

(ii) Include a requirement in the regulations proposed pursuant to subsection 4.2(c)(i) of this section that United States IaaS Providers prohibit any foreign reseller of their United States IaaS Product from providing those products unless such foreign reseller submits to the United States IaaS

Provider a report, which the United States IaaS Provider must provide to the Secretary of Commerce, detailing each instance in which a foreign person transacts with the foreign reseller to use the United States IaaS Product to conduct a training run described in subsection 4.2(c)(i) of this section. Such reports shall include, at a minimum, the information specified in subsection 4.2(c)(i) of this section as well as any additional information identified by the Secretary.

(iii) Determine the set of technical conditions for a large AI model to have potential capabilities that could be used in malicious cyber-enabled activity, and revise that determination as necessary and appropriate. Until the Secretary makes such a determination, a model shall be considered to have potential capabilities that could be used in malicious cyber-enabled activity if it requires a quantity of computing power greater than 10^{26} integer or floating-point operations and is trained on a computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum compute capacity of 10^{20} integer or floating-point operations per second for training AI.

(d) Within 180 days of the date of this order, pursuant to the finding set forth in subsection 4.2(c) of this section, the Secretary of Commerce shall propose regulations that require United States IaaS Providers to ensure that foreign resellers of United States IaaS Products verify the identity of any foreign person that obtains an IaaS account (account) from the foreign reseller. These regulations shall, at a minimum:

(i) Set forth the minimum standards that a United States IaaS Provider must require of foreign resellers of its United States IaaS Products to verify the identity of a foreign person who opens an account or maintains an existing account with a foreign reseller, including:

(A) the types of documentation and procedures that foreign resellers of United States IaaS Products must require to verify the identity of any foreign person acting as a lessee or sub-lessee of these products or services;

(B) records that foreign resellers of United States IaaS Products must securely maintain regarding a foreign person that obtains an account, including information establishing:

(1) the identity of such foreign person, including name and address;

(2) the means and source of payment (including any associated financial institution and other identifiers such as credit card number, account number, customer identifier, transaction identifiers, or virtual currency wallet or wallet address identifier);

(3) the electronic mail address and telephonic contact information used to verify a foreign person's identity; and

(4) the Internet Protocol addresses used for access or administration and the date and time of each such access or administrative action related to ongoing verification of such foreign person's ownership of such an account; and

(C) methods that foreign resellers of United States IaaS Products must implement to limit all third-party access to the information described in this subsection, except insofar as such access is otherwise consistent with this order and allowed under applicable law;

(ii) Take into consideration the types of accounts maintained by foreign resellers of United States IaaS Products, methods of opening an account, and types of identifying information available to accomplish the objectives of identifying foreign malicious cyber actors using any such products and avoiding the imposition of an undue burden on such resellers; and

(iii) Provide that the Secretary of Commerce, in accordance with such standards and procedures as the Secretary may delineate and in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, may exempt a United States IaaS Provider with respect to any specific foreign reseller of their United States IaaS Products, or with respect to any specific type of account or lessee, from the requirements of any regulation issued pursuant to this subsection. Such standards and procedures may include a finding by the Secretary that such foreign reseller, account, or lessee complies with security best practices to otherwise deter abuse of United States IaaS Products.

(e) The Secretary of Commerce is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by the International Emergency Economic Powers Act, 50 U.S.C. 1701 *et seq.*, as may be necessary to carry out the purposes of subsections 4.2(c) and (d) of this section. Such actions may include a requirement that United States IaaS Providers require foreign resellers of United States IaaS Products to provide United States IaaS Providers verifications relative to those subsections.

4.3. Managing AI in Critical Infrastructure and in Cybersecurity. (a) To ensure the protection of critical
infrastructure, the following actions shall be taken:

(i) Within 90 days of the date of this order, and at least annually thereafter, the head of each agency with relevant regulatory authority over critical infrastructure and the heads of relevant SRMAs, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security for consideration of cross-sector risks, shall evaluate and provide to the Secretary of Homeland Security an assessment of potential risks related to the use of AI in critical infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber attacks, and shall consider ways to mitigate these vulnerabilities. Independent regulatory agencies are encouraged, as they deem appropriate, to contribute to sector-specific risk assessments.

(ii) Within 150 days of the date of this order, the Secretary of the Treasury shall issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks.

(iii) Within 180 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of Commerce and with SRMAs and other regulators as determined by the Secretary of Homeland Security, shall incorporate as appropriate the AI Risk Management Framework, NIST AI 100-1, as well as other appropriate security guidance, into relevant safety and security guidelines for use by critical infrastructure owners and operators.

(iv) Within 240 days of the completion of the guidelines described in subsection 4.3(a)(iii) of this section, the Assistant to the President for National Security Affairs and the Director of OMB, in consultation with the Secretary of Homeland Security, shall coordinate work by the heads of agencies with authority over critical infrastructure to develop and take steps for the Federal Government to mandate such guidelines, or appropriate portions thereof, through regulatory or other appropriate action. Independent regulatory agencies are encouraged, as they deem appropriate, to consider whether to mandate guidance through regulatory action in their areas of authority and responsibility.

(v) The Secretary of Homeland Security shall establish an Artificial Intelligence Safety and Security Board as an advisory committee pursuant to section 871 of the Homeland Security Act of 2002 (Public Law 107-296). The Advisory Committee shall include AI experts from the private sector, academia, and government, as appropriate, and provide to the Secretary of Homeland Security and the Federal Government's critical infrastructure community advice, information, or recommendations for improving security, resilience, and incident response related to AI usage in critical infrastructure.

(b) To capitalize on AI's potential to improve United States cyber defenses:

(i) The Secretary of Defense shall carry out the actions described in subsections 4.3(b)(ii) and (iii) of this section for national security systems, and the Secretary of Homeland Security shall carry out these actions for non-national security systems. Each shall do so in consultation with the heads of other relevant agencies as the Secretary of Defense and the Secretary of Homeland Security may deem appropriate.

(ii) As set forth in subsection 4.3(b)(i) of this section, within 180 days of the date of this order, the Secretary of Defense and the Secretary of Homeland Security shall, consistent with applicable law, each develop plans for, conduct, and complete an operational pilot project to identify, develop, test, evaluate, and deploy AI capabilities, such as large-language models, to aid in the discovery and remediation of vulnerabilities in critical United States Government software, systems, and networks.

(iii) As set forth in subsection 4.3(b)(i) of this section, within 270 days of the date of this order, the Secretary of Defense and the Secretary of Homeland Security shall each provide a report to the Assistant to the President for National Security Affairs on the results of actions taken pursuant to the plans and operational pilot projects required by subsection 4.3(b)(ii) of this section, including a description of any vulnerabilities found and fixed through the development and deployment of AI capabilities and any lessons learned on how to identify, develop, test, evaluate, and deploy AI capabilities effectively for cyber defense.

4.4. Reducing Risks at the Intersection of AI and CBRN Threats. (a) To better understand and mitigate the risk of AI being misused to assist in the development or use of CBRN threats — with a particular focus on biological weapons — the following actions shall be taken:

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Energy and the Director of the Office of Science and Technology Policy (OSTP), shall evaluate the potential for AI to be misused to enable the development or production of CBRN threats, while also considering the benefits and application of AI to counter these threats, including, as appropriate, the results of work conducted under section 8(b) of this order. The Secretary of Homeland Security shall:

(A) consult with experts in AI and CBRN issues from the Department of Energy, private AI laboratories, academia, and third-party model evaluators, as appropriate, to evaluate AI model capabilities to present CBRN threats — for the sole purpose of guarding against those threats — as well as options for minimizing the risks of AI model misuse to generate or exacerbate those threats; and

(B) submit a report to the President that describes the progress of these efforts, including an assessment of the types of AI models that may present CBRN risks to the United States, and that makes recommendations for regulating or overseeing the training, deployment, publication, or use of these models, including requirements for safety evaluations and guardrails for mitigating potential threats to national security.

(ii) Within 120 days of the date of this order, the Secretary of Defense, in consultation with the Assistant to the President for National Security

Affairs and the Director of OSTP, shall enter into a contract with the National Academies of Sciences, Engineering, and Medicine to conduct — and submit to the Secretary of Defense, the Assistant to the President for National Security Affairs, the Director of the Office of Pandemic Preparedness and Response Policy, the Director of OSTP, and the Chair of the Chief Data Officer Council — a study that:

(A) assesses the ways in which AI can increase biosecurity risks, including risks from generative AI models trained on biological data, and makes recommendations on how to mitigate these risks;

(B) considers the national security implications of the use of data and datasets, especially those associated with pathogens and omics studies, that the United States Government hosts, generates, funds the creation of, or otherwise owns, for the training of generative AI models, and makes recommendations on how to mitigate the risks related to the use of these data and datasets;

(C) assesses the ways in which AI applied to biology can be used to reduce biosecurity risks, including recommendations on opportunities to coordinate data and high-performance computing resources; and

(D) considers additional concerns and opportunities at the intersection of AI and synthetic biology that the Secretary of Defense deems appropriate.

(b) To reduce the risk of misuse of synthetic nucleic acids, which could be substantially increased by AI's capabilities in this area, and improve biosecurity measures for the nucleic acid synthesis industry, the following actions shall be taken:

(i) Within 180 days of the date of this order, the Director of OSTP, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Health and Human Services (HHS), the Secretary of Energy, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other relevant agencies as the Director of OSTP may deem appropriate, shall establish a framework, incorporating, as appropriate, existing United States Government guidance, to encourage providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms, including standards and recommended incentives. As part of this framework, the Director of OSTP shall:

(A) establish criteria and mechanisms for ongoing identification of biological sequences that could be used in a manner that would pose a risk to the national security of the United States; and

(B) determine standardized methodologies and tools for conducting and verifying the performance of sequence synthesis procurement screening, including customer screening approaches to support due diligence with respect to managing security risks posed by purchasers of biological sequences identified in subsection 4.4(b)(i)(A) of this section, and processes for the reporting of concerning activity to enforcement entities.

(ii) Within 180 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in coordination with the Director of OSTP, and in consultation with the Secretary of State, the Secretary of HHS, and the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall initiate an effort to engage with industry and relevant stakeholders, informed by the framework developed under subsection 4.4(b)(i) of this section, to develop and refine for possible use by synthetic nucleic acid sequence providers:

(A) specifications for effective nucleic acid synthesis procurement screening;

(B) best practices, including security and access controls, for managing sequence-of-concern databases to support such screening;

(C) technical implementation guides for effective screening; and

(D) conformity-assessment best practices and mechanisms.

(iii) Within 180 days of the establishment of the framework pursuant to subsection 4.4(b)(i) of this section, all agencies that fund life-sciences research shall, as appropriate and consistent with applicable law, establish that, as a requirement of funding, synthetic nucleic acid procurement is conducted through providers or manufacturers that adhere to the framework, such as through an attestation from the provider or manufacturer. The Assistant to the President for National Security Affairs and the Director of OSTP shall coordinate the process of reviewing such funding requirements to facilitate consistency in implementation of the framework across funding agencies.

(iv) In order to facilitate effective implementation of the measures described in subsections 4.4(b)(i)-(iii) of this section, the Secretary of Homeland Security, in consultation with the heads of other relevant agencies as the Secretary of Homeland Security may deem appropriate, shall:

(A) within 180 days of the establishment of the framework pursuant to subsection 4.4(b)(i) of this section, develop a framework to conduct structured evaluation and stress testing of nucleic acid synthesis procurement screening, including the systems developed in accordance with subsections 4.4(b)(i)-(ii) of this section and implemented by providers of synthetic nucleic acid sequences; and

(B) following development of the framework pursuant to subsection 4.4(b)(iv)(A) of this section, submit an annual report to the Assistant to the President for National Security Affairs, the Director of the Office of Pandemic Preparedness and Response Policy, and the Director of OSTP on any results of the activities conducted pursuant to subsection 4.4(b)(iv)(A) of this section, including recommendations, if any, on how to strengthen nucleic acid synthesis procurement screening, including customer screening systems.

4.5. Reducing the Risks Posed by Synthetic Content.

To foster capabilities for identifying and labeling synthetic content produced by AI systems, and to establish the authenticity and provenance of digital content, both synthetic and not synthetic, produced by the Federal Government or on its behalf:

(a) Within 240 days of the date of this order, the Secretary of Commerce, in consultation with the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall submit a report to the Director of OMB and the Assistant to the President for National Security Affairs identifying the existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for:

(i) authenticating content and tracking its provenance;

(ii) labeling synthetic content, such as using watermarking;

(iii) detecting synthetic content;

(iv) preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual);

(v) testing software used for the above purposes; and

(vi) auditing and maintaining synthetic content.

(b) Within 180 days of submitting the report required under subsection 4.5(a) of this section, and updated periodically thereafter, the Secretary of Commerce, in coordination with the Director of OMB, shall develop guidance regarding the existing tools and practices for digital content authentication and synthetic content detection measures. The guidance shall include measures for the purposes listed in subsection 4.5(a) of this section.

(c) Within 180 days of the development of the guidance required under subsection 4.5(b) of this section, and updated periodically thereafter, the Director of OMB, in consultation with the Secretary of State; the Secretary of Defense; the Attorney General; the Secretary of Commerce, acting through the Director of NIST; the Secretary of Homeland Security; the Director of National Intelligence; and the heads of other agencies that the Director of OMB deems appropriate, shall — for the purpose of strengthening public confidence in the integrity of official United States Government digital content — issue guidance to agencies for labeling and authenticating such content that they produce or publish.

(d) The Federal Acquisition Regulatory Council shall, as appropriate and consistent with applicable law, consider amending the Federal Acquisition Regulation to take into account the guidance established under subsection 4.5 of this section.

4.6. Soliciting Input on Dual-Use Foundation Models with Widely Available Model Weights. When the weights for a dual-use foundation model are widely available — such as when they are publicly posted on the Internet — there can be substantial benefits to innovation, but also substantial security risks, such as the removal of safeguards within the model. To address the risks and potential benefits of dual-use foundation models with widely available weights, within 270 days of the date of this order, the Secretary of Commerce, acting through the Assistant Secretary of Commerce for Communications and Information, and in consultation with the Secretary of State, shall:

(a) solicit input from the private sector, academia, civil society, and other stakeholders through a public consultation process on potential risks, benefits, other implications, and appropriate policy and regulatory approaches related to dual-use foundation models for which the model weights are widely available, including:

(i) risks associated with actors fine-tuning dual-use foundation models for which the model weights are widely available or removing those models' safeguards;

(ii) benefits to AI innovation and research, including research into AI safety and risk management, of dual-use foundation models for which the model weights are widely available; and

(iii) potential voluntary, regulatory, and international mechanisms to manage the risks and maximize the benefits of dual-use foundation models for which the model weights are widely available; and

(b) based on input from the process described in subsection 4.6(a) of this section, and in consultation with the heads of other relevant agencies as the

Secretary of Commerce deems appropriate, submit a report to the President on the potential benefits, risks, and implications of dual-use foundation models for which the model weights are widely available, as well as policy and regulatory recommendations pertaining to those models.

4.7. Promoting Safe Release and Preventing the Malicious Use of Federal Data for AI Training.To improve public data access and manage security risks, and consistent with the objectives of the Open, Public, Electronic, and Necessary Government Data Act (title II of Public Law 115-435) to expand public access to Federal data assets in a machine-readable format while also taking into account security considerations, including the risk that information in an individual data asset in isolation does not pose a security risk but, when combined with other available information, may pose such a risk:

(a) within 270 days of the date of this order, the Chief Data Officer Council, in consultation with the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, and the Director of National Intelligence, shall develop initial guidelines for performing security reviews, including reviews to identify and manage the potential security risks of releasing Federal data that could aid in the development of CBRN weapons as well as the development of autonomous offensive cyber capabilities, while also providing public access to Federal Government data in line with the goals stated in the Open, Public, Electronic, and Necessary Government Data Act (title II of Public Law 115-435); and

(b) within 180 days of the development of the initial guidelines required by subsection 4.7(a) of this section, agencies shall conduct a security review of all data assets in the comprehensive data inventory required under 44 U.S.C. 3511(a)(1) and (2)(B) and shall take steps, as appropriate and consistent with applicable law, to address the highest-priority potential security risks that releasing that data could raise with respect to CBRN weapons, such as the ways in which that data could be used to train AI systems.

4.8. Directing the Development of a National Security Memorandum. To develop a coordinated executive branch approach to managing AI's security risks, the Assistant to the President for National Security Affairs and the Assistant to the President and Deputy Chief of Staff for Policy shall oversee an interagency process with the purpose of, within 270 days of the date of this order, developing and submitting a proposed National Security Memorandum on AI to the President. The memorandum shall address the governance of AI used as a component of a national security system or for military and intelligence purposes. The memorandum shall take into account current efforts to govern the development and use of AI for national security systems. The memorandum shall outline actions for the Department of Defense, the Department of State, other relevant agencies, and the Intelligence Community to address the national security risks and potential benefits posed by AI. In particular, the memorandum shall:

(a) provide guidance to the Department of Defense, other relevant agencies, and the Intelligence Community on the continued adoption of AI capabilities to advance the United States national security mission, including through directing specific AI assurance and risk-management practices for national security uses of AI that may affect the rights or safety of United States persons and, in appropriate contexts, non-United States persons; and

(b) direct continued actions, as appropriate and consistent with applicable law, to address the potential use of AI systems by adversaries and other foreign actors in ways that threaten the capabilities or objectives of the Department of Defense or the Intelligence Community, or that otherwise pose risks to the security of the United States or its allies and partners.

Sec. 5. Promoting Innovation and Competition.

5.1. Attracting AI Talent to the United States. (a) Within 90 days of the date of this order, to attract and retain talent in AI and other critical and emerging technologies in the United States economy, the Secretary of State and the Secretary of Homeland Security shall take appropriate steps to:

(i) streamline processing times of visa petitions and applications, including by ensuring timely availability of visa appointments, for noncitizens who seek to travel to the United States to work on, study, or conduct research in AI or other critical and emerging technologies; and

(ii) facilitate continued availability of visa appointments in sufficient volume for applicants with expertise in AI or other critical and emerging technologies.

(b) Within 120 days of the date of this order, the Secretary of State shall:

(i) consider initiating a rulemaking to establish new criteria to designate countries and skills on the Department of State's Exchange Visitor Skills List as it relates to the 2-year foreign residence requirement for certain J-1 nonimmigrants, including those skills that are critical to the United States;

(ii) consider publishing updates to the 2009 Revised Exchange Visitor Skills List (74 FR 20108); and

(iii) consider implementing a domestic visa renewal program under 22 C.F.R. 41.111(b) to facilitate the ability of qualified applicants, including highly skilled talent in AI and critical and emerging technologies, to continue their work in the United States without unnecessary interruption.

(c) Within 180 days of the date of this order, the Secretary of State shall:

(i) consider initiating a rulemaking to expand the categories of nonimmigrants who qualify for the domestic visa renewal program covered under 22 C.F.R. 41.111(b) to include academic J-1 research scholars and F-1 students in science, technology, engineering, and mathematics (STEM); and

(ii) establish, to the extent permitted by law and available appropriations, a program to identify and attract top talent in AI and other critical and emerging technologies at universities, research institutions, and the private sector overseas, and to establish and increase connections with that talent to educate them on opportunities and resources for research and employment in the United States, including overseas educational components to inform top STEM talent of nonimmigrant and immigrant visa options and potential expedited adjudication of their visa petitions and applications.

(d) Within 180 days of the date of this order, the Secretary of Homeland Security shall:

(i) review and initiate any policy changes the Secretary determines necessary and appropriate to clarify and modernize immigration pathways for experts in AI and other critical and emerging technologies, including O-1A and EB-1 noncitizens of extraordinary ability; EB-2 advanced-degree holders and noncitizens of exceptional ability; and startup founders in AI and other critical and emerging technologies using the International Entrepreneur Rule; and

(ii) continue its rulemaking process to modernize the H-1B program and enhance its integrity and usage, including by experts in AI and other critical and emerging technologies, and consider initiating a rulemaking to enhance the process for noncitizens, including experts in AI and other critical and emerging technologies and their spouses, dependents, and children, to adjust their status to lawful permanent resident.

(e) Within 45 days of the date of this order, for purposes of considering updates to the "Schedule A" list of occupations, 20 C.F.R. 656.5, the Secretary of Labor shall publish a request for information (RFI) to solicit public input, including from industry and worker-advocate communities, identifying AI and other STEM-related occupations, as well as additional occupations across the economy, for which there is an insufficient number of ready, willing, able, and qualified United States workers.

(f) The Secretary of State and the Secretary of Homeland Security shall, consistent with applicable law and implementing regulations, use their discretionary authorities to support and attract foreign nationals with special skills in AI and other critical and emerging technologies seeking to work, study, or conduct research in the United States.

(g) Within 120 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of OSTP, shall develop and publish informational resources to better attract and retain experts in AI and other critical and emerging technologies, including:

(i) a clear and comprehensive guide for experts in AI and other critical and emerging technologies to understand their options for working in the United States, to be published in multiple relevant languages on AI.gov; and

(ii) a public report with relevant data on applications, petitions, approvals, and other key indicators of how experts in AI and other critical and emerging technologies have utilized the immigration system through the end of Fiscal Year 2023.

5.2. Promoting Innovation. (a) To develop and strengthen public-private partnerships for advancing innovation, commercialization, and risk-mitigation methods for AI, and to help promote safe, responsible, fair, privacy-protecting, and trustworthy AI systems, the Director of NSF shall take the following steps:

(i) Within 90 days of the date of this order, in coordination with the heads of agencies that the Director of NSF deems appropriate, launch a pilot program implementing the National AI Research Resource (NAIRR), consistent with past recommendations of the NAIRR Task Force. The program shall pursue the infrastructure, governance mechanisms, and user interfaces to pilot an initial integration of distributed computational, data, model, and training resources to be made available to the research community in support of AI-related research and development. The Director of NSF shall identify Federal and private sector computational, data, software, and training resources appropriate for inclusion in the NAIRR pilot program. To assist with such work, within 45 days of the date of this order, the heads of agencies whom the Director of NSF identifies for coordination pursuant to this subsection shall each submit to the Director of NSF a report identifying the agency resources that could be developed and integrated into such a pilot program. These reports shall include a description of such resources, including their current status and availability; their format, structure, or technical specifications; associated agency expertise that will be provided; and the benefits and risks associated with their inclusion in the NAIRR pilot program. The heads of independent regulatory agencies are encouraged to take similar steps, as they deem appropriate.

(ii) Within 150 days of the date of this order, fund and launch at least one NSF Regional Innovation Engine that prioritizes AI-related work, such as AI-related research, societal, or workforce needs.

(iii) Within 540 days of the date of this order, establish at least four new National AI Research Institutes, in addition to the 25 currently funded as of the date of this order.

(b) Within 120 days of the date of this order, to support activities involving high-performance and data-intensive computing, the Secretary of Energy, in coordination with the Director of NSF, shall, in a manner consistent with applicable law and available appropriations, establish a pilot program to enhance existing successful training programs for scientists, with the goal of training 500 new researchers by 2025 capable of meeting the rising demand for AI talent.

(c) To promote innovation and clarify issues related to AI and inventorship of patentable subject matter, the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO Director) shall:

(i) within 120 days of the date of this order, publish guidance to USPTO patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed;

(ii) subsequently, within 270 days of the date of this order, issue additional guidance to USPTO patent examiners and applicants to address other considerations at the intersection of AI and IP, which could include, as the USPTO Director deems necessary, updated guidance on patent eligibility to address innovation in AI and critical and emerging technologies; and

(iii) within 270 days of the date of this order or 180 days after the United States Copyright Office of the Library of Congress publishes its forthcoming AI study that will address copyright issues raised by AI, whichever comes later, consult with the Director of the United States Copyright Office and issue recommendations to the President on potential executive actions relating to copyright and AI. The recommendations shall address any copyright and related issues discussed in the United States Copyright Office's study, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training.

(d) Within 180 days of the date of this order, to assist developers of AI in combatting AI-related IP risks, the Secretary of Homeland Security, acting through the Director of the National Intellectual Property Rights Coordination Center, and in consultation with the Attorney General, shall develop a training, analysis, and evaluation program to mitigate AI-related IP risks. Such a program shall:

(i) include appropriate personnel dedicated to collecting and analyzing reports of AI-related IP theft, investigating such incidents with implications for national security, and, where appropriate and consistent with applicable law, pursuing related enforcement actions;

(ii) implement a policy of sharing information and coordinating on such work, as appropriate and consistent with applicable law, with the Federal Bureau of Investigation; United States Customs and Border Protection; other agencies; State and local agencies; and appropriate international organizations, including through work-sharing agreements;

(iii) develop guidance and other appropriate resources to assist private sector actors with mitigating the risks of AI-related IP theft;

(iv) share information and best practices with AI developers and law enforcement personnel to identify incidents, inform stakeholders of current legal requirements, and evaluate AI systems for IP law violations, as well as develop mitigation strategies and resources; and

(v) assist the Intellectual Property Enforcement Coordinator in updating the Intellectual Property Enforcement Coordinator Joint Strategic Plan on Intellectual Property Enforcement to address AI-related issues.

(e) To advance responsible AI innovation by a wide range of healthcare technology developers that promotes the welfare of patients and workers in the healthcare sector, the Secretary of HHS shall identify and, as appropriate and consistent with applicable law and the activities directed in section 8 of this order, prioritize grantmaking and other awards, as well as undertake related efforts, to support responsible AI development and use, including:

(i) collaborating with appropriate private sector actors through HHS programs that may support the advancement of AI-enabled tools that develop personalized immune-response profiles for patients, consistent with section 4 of this order;

(ii) prioritizing the allocation of 2024 Leading Edge Acceleration Project cooperative agreement awards to initiatives that explore ways to improve healthcare-data quality to support the responsible development of AI tools for clinical care, real-world-evidence programs, population health, public health, and related research; and

(iii) accelerating grants awarded through the National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity (AIM-AHEAD) program and showcasing current AIM-AHEAD activities in underserved communities.

(f) To advance the development of AI systems that improve the quality of veterans' healthcare, and in order to support small businesses' innovative capacity, the Secretary of Veterans Affairs shall:

(i) within 365 days of the date of this order, host two 3-month nationwide AI Tech Sprint competitions; and

(ii) as part of the AI Tech Sprint competitions and in collaboration with appropriate partners, provide participants access to technical assistance, mentorship opportunities, individualized expert feedback on products under development, potential contract opportunities, and other programming and resources.

(g) Within 180 days of the date of this order, to support the goal of strengthening our Nation's resilience against climate change impacts and building an equitable clean energy economy for the future, the Secretary of Energy, in consultation with the Chair of the Federal Energy Regulatory Commission, the Director of OSTP, the Chair of the Council on Environmental Quality, the Assistant to the President and National Climate Advisor, and the heads of other relevant agencies as the Secretary of Energy may deem appropriate, shall:

(i) issue a public report describing the potential for AI to improve planning, permitting, investment, and operations for electric grid infrastructure and to enable the provision of clean, affordable, reliable, resilient, and secure electric power to all Americans;

(ii) develop tools that facilitate building foundation models useful for basic and applied science, including models that streamline permitting and environmental reviews while improving environmental and social outcomes;

(iii) collaborate, as appropriate, with private sector organizations and members of academia to support development of AI tools to mitigate climate change risks;

(iv) take steps to expand partnerships with industry, academia, other agencies, and international allies and partners to utilize the Department of Energy's computing capabilities and AI testbeds to build foundation models that support new applications in science and energy, and for national security, including partnerships that increase community preparedness for climate-related risks, enable clean-energy deployment (including addressing delays in permitting reviews), and enhance grid reliability and resilience; and

(v) establish an office to coordinate development of AI and other critical and emerging technologies across Department of Energy programs and the 17 National Laboratories.

(h) Within 180 days of the date of this order, to understand AI's implications for scientific research, the President's Council of Advisors on Science and Technology shall submit to the President and make publicly available a report on the potential role of AI, especially given recent developments in AI, in research aimed at tackling major societal and global challenges. The report shall include a discussion of issues that may hinder the effective use of AI in research and practices needed to ensure that AI is used responsibly for research.

5.3. Promoting Competition. (a) The head of each agency developing policies and regulations related to AI shall use their authorities, as appropriate and consistent with applicable law, to promote competition in AI and related technologies, as well as in other markets. Such actions include addressing risks arising from concentrated control of key inputs, taking steps to stop unlawful collusion and prevent dominant firms from disadvantaging competitors, and working to provide new opportunities for small businesses and entrepreneurs. In particular, the Federal Trade Commission is encouraged to consider, as it deems appropriate, whether to exercise the Commission's existing authorities, including its rulemaking authority under the Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*, to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI.

(b) To promote competition and innovation in the semiconductor industry, recognizing that semiconductors power AI technologies and that their availability is critical to AI competition, the Secretary of Commerce shall, in implementing division A of Public Law 117-167, known as the

Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022, promote competition by:

(i) implementing a flexible membership structure for the National Semiconductor Technology Center that attracts all parts of the semiconductor and microelectronics ecosystem, including startups and small firms;

(ii) implementing mentorship programs to increase interest and participation in the semiconductor industry, including from workers in underserved communities;

(iii) increasing, where appropriate and to the extent permitted by law, the availability of resources to startups and small businesses, including:

(A) funding for physical assets, such as specialty equipment or facilities, to which startups and small businesses may not otherwise have access;

(B) datasets — potentially including test and performance data — collected, aggregated, or shared by CHIPS research and development programs;

(C) workforce development programs;

(D) design and process technology, as well as IP, as appropriate; and

(E) other resources, including technical and intellectual property assistance, that could accelerate commercialization of new technologies by startups and small businesses, as appropriate; and

(iv) considering the inclusion, to the maximum extent possible, and as consistent with applicable law, of competition-increasing measures in notices of funding availability for commercial research-and-development facilities focused on semiconductors, including measures that increase access to facility capacity for startups or small firms developing semiconductors used to power AI technologies.

(c) To support small businesses innovating and commercializing AI, as well as in responsibly adopting and deploying AI, the Administrator of the

Small Business Administration shall:

(i) prioritize the allocation of Regional Innovation Cluster program funding for clusters that support planning activities related to the establishment of one or more Small Business AI Innovation and Commercialization Institutes that provide support, technical assistance, and other resources to small businesses seeking to innovate, commercialize, scale, or otherwise advance the development of AI;

(ii) prioritize the allocation of up to $2 million in Growth Accelerator Fund Competition bonus prize funds for accelerators that support the incorporation or expansion of AI-related curricula, training, and technical assistance, or other AI-related resources within their programming; and

(iii) assess the extent to which the eligibility criteria of existing programs, including the State Trade Expansion Program, Technical and Business Assistance funding, and capital-access programs — such as the 7(a) loan program, 504 loan program, and Small Business Investment Company (SBIC) program — support appropriate expenses by small businesses related to the adoption of AI and, if feasible and appropriate, revise eligibility criteria to improve support for these expenses.

(d) The Administrator of the Small Business Administration, in coordination with resource partners, shall conduct outreach regarding, and raise awareness of, opportunities for small businesses to use capital-access programs described in subsection 5.3(c) of this section for eligible AI-related purposes, and for eligible investment funds with AI-related expertise — particularly those seeking to serve or with experience serving underserved communities — to apply for an SBIC license.

Sec. 6. Supporting Workers.(a) To advance the Government's understanding of AI's implications for workers, the following actions shall be taken within 180 days of the date of this order:

(i) The Chairman of the Council of Economic Advisers shall prepare and submit a report to the President on the labor-market effects of AI.

(ii) To evaluate necessary steps for the Federal Government to address AI-related workforce disruptions, the Secretary of Labor shall submit to the President a report analyzing the abilities of agencies to support workers displaced by the adoption of AI and other technological advancements. The report shall, at a minimum:

(A) assess how current or formerly operational Federal programs designed to assist workers facing job disruptions — including unemployment insurance and programs authorized by the Workforce Innovation and Opportunity Act (Public Law 113-128) — could be used to respond to possible future AI-related disruptions; and

(B) identify options, including potential legislative measures, to strengthen or develop additional Federal support for workers displaced by AI and, in consultation with the Secretary of Commerce and the Secretary of Education, strengthen and expand education and training opportunities that provide individuals pathways to occupations related to AI.

(b) To help ensure that AI deployed in the workplace advances employees' well-being:

(i) The Secretary of Labor shall, within 180 days of the date of this order and in consultation with other agencies and with outside entities, including labor unions and workers, as the Secretary of Labor deems appropriate, develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits. The principles and best practices shall include specific steps for employers to take with regard to AI, and shall cover, at a minimum:

(A) job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers;

(B) labor standards and job quality, including issues related to the equity, protected-activity, compensation, health, and safety implications of AI in the workplace; and

(C) implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management, and activity protected under worker-protection laws.

(ii) After principles and best practices are developed pursuant to subsection (b)(i) of this section, the heads of agencies shall consider, in consultation with the Secretary of Labor, encouraging the adoption of these guidelines in their programs to the extent appropriate for each program and consistent with applicable law.

(iii) To support employees whose work is monitored or augmented by AI in being compensated appropriately for all of their work time, the Secretary of Labor shall issue guidance to make clear that employers that deploy AI to monitor or augment employees' work must continue to comply with protections that ensure that workers are compensated for their hours worked, as defined under the Fair Labor Standards Act of 1938, 29 U.S.C. 201 *et seq.*, and other legal requirements.

(c) To foster a diverse AI-ready workforce, the Director of NSF shall prioritize available resources to support AI-related education and AI-related workforce development through existing programs. The Director shall additionally consult with agencies, as appropriate, to identify further opportunities for agencies to allocate resources for those purposes. The actions by the Director shall use appropriate fellowship programs and awards for these purposes.

Sec. 7. Advancing Equity and Civil Rights.

7.1. Strengthening AI and Civil Rights in the Criminal Justice System. (a) To address unlawful discrimination and other harms that may be exacerbated by AI, the Attorney General shall:

(i) consistent with Executive Order 12250 of November 2, 1980 (Leadership and Coordination of Nondiscrimination Laws), Executive Order 14091, and 28 C.F.R. 0.50-51, coordinate with and support agencies in their implementation and enforcement of existing Federal laws to address civil rights and civil liberties violations and discrimination related to AI;

(ii) direct the Assistant Attorney General in charge of the Civil Rights Division to convene, within 90 days of the date of this order, a meeting of the heads of Federal civil rights offices — for which meeting the heads of civil rights offices within independent regulatory agencies will be encouraged to join — to discuss comprehensive use of their respective authorities and offices to: prevent and address discrimination in the use of automated systems, including algorithmic discrimination; increase coordination between the Department of Justice's Civil Rights Division and Federal civil rights offices concerning issues related to AI and algorithmic discrimination; improve external stakeholder engagement to promote public awareness of potential discriminatory uses and effects of AI; and develop, as appropriate, additional training, technical assistance, guidance, or other resources; and

(iii) consider providing, as appropriate and consistent with applicable law, guidance, technical assistance, and training to State, local, Tribal, and territorial investigators and prosecutors on best practices for investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI.

(b) To promote the equitable treatment of individuals and adhere to the Federal Government's fundamental obligation to ensure fair and impartial justice for all, with respect to the use of AI in the criminal justice system, the Attorney General shall, in consultation with the Secretary of Homeland Security and the Director of OSTP:

(i) within 365 days of the date of this order, submit to the President a report that addresses the use of AI in the criminal justice system, including any use in:

(A) sentencing;

(B) parole, supervised release, and probation;

(C) bail, pretrial release, and pretrial detention;

(D) risk assessments, including pretrial, earned time, and early release or transfer to home-confinement determinations;

(E) police surveillance;

(F) crime forecasting and predictive policing, including the ingestion of historical crime data into AI systems to predict high-density "hot spots";

(G) prison-management tools; and

(H) forensic analysis;

(ii) within the report set forth in subsection 7.1(b)(i) of this section:

(A) identify areas where AI can enhance law enforcement efficiency and accuracy, consistent with protections for privacy, civil rights, and civil liberties; and

(B) recommend best practices for law enforcement agencies, including safeguards and appropriate use limits for AI, to address the concerns set forth in section 13(e)(i) of Executive Order 14074 as well as the best practices and the guidelines set forth in section 13(e)(iii) of Executive Order 14074; and

(iii) supplement the report set forth in subsection 7.1(b)(i) of this section as appropriate with recommendations to the President, including with respect to requests for necessary legislation.

(c) To advance the presence of relevant technical experts and expertise (such as machine-learning engineers, software and infrastructure engineering, data privacy experts, data scientists, and user experience researchers) among law enforcement professionals:

(i) The interagency working group created pursuant to section 3 of Executive Order 14074 shall, within 180 days of the date of this order, identify and share best practices for recruiting and hiring law enforcement professionals who have the technical skills mentioned in subsection 7.1(c) of this section, and for training law enforcement professionals about responsible application of AI.

(ii) Within 270 days of the date of this order, the Attorney General shall, in consultation with the Secretary of Homeland Security, consider those best practices and the guidance developed under section 3(d) of Executive Order 14074 and, if necessary, develop additional general recommendations for State, local, Tribal, and territorial law enforcement agencies and criminal justice agencies seeking to recruit, hire, train, promote, and retain highly qualified and service-oriented officers and staff with relevant technical knowledge. In considering this guidance, the Attorney General shall consult with State, local, Tribal, and territorial law enforcement agencies, as appropriate.

(iii) Within 365 days of the date of this order, the Attorney General shall review the work conducted pursuant to section 2(b) of Executive Order

14074 and, if appropriate, reassess the existing capacity to investigate law enforcement deprivation of rights under color of law resulting from the use of AI, including through improving and increasing training of Federal law enforcement officers, their supervisors, and Federal prosecutors on how to investigate and prosecute cases related to AI involving the deprivation of rights under color of law pursuant to 18 U.S.C. 242.

7.2. Protecting Civil Rights Related to Government Benefits and Programs. (a) To advance equity and civil rights, consistent with the directives of Executive Order 14091, and in addition to complying with the guidance on Federal Government use of AI issued pursuant to section 10.1(b) of this order, agencies shall use their respective civil rights and civil liberties offices and authorities — as appropriate and consistent with applicable law — to prevent and address unlawful discrimination and other harms that result from uses of AI in Federal Government programs and benefits administration. This directive does not apply to agencies' civil or criminal enforcement authorities. Agencies shall consider opportunities to ensure that their respective civil rights and civil liberties offices are appropriately consulted on agency decisions regarding the design, development, acquisition, and use of AI in Federal Government programs and benefits administration. To further these objectives, agencies shall also consider opportunities to increase coordination, communication, and engagement about AI as appropriate with community-based organizations; civil-rights and civil-liberties organizations; academic institutions; industry; State, local, Tribal, and territorial governments; and other stakeholders.

(b) To promote equitable administration of public benefits:

(i) The Secretary of HHS shall, within 180 days of the date of this order and in consultation with relevant agencies, publish a plan, informed by the guidance issued pursuant to section 10.1(b) of this order, addressing the use of automated or algorithmic systems in the implementation by States and localities of public benefits and services administered by the Secretary, such as to promote: assessment of access to benefits by qualified recipients; notice to recipients about the presence of such systems; regular evaluation to detect unjust denials; processes to retain appropriate levels of discretion of expert agency staff; processes to appeal denials to human reviewers; and analysis of whether algorithmic systems in use by benefit programs achieve equitable and just outcomes.

(ii) The Secretary of Agriculture shall, within 180 days of the date of this order and as informed by the guidance issued pursuant to section 10.1(b) of this order, issue guidance to State, local, Tribal, and territorial public-benefits administrators on the use of automated or algorithmic systems in implementing benefits or in providing customer support for benefit programs administered by the Secretary, to ensure that programs using those systems:

(A) maximize program access for eligible recipients;

(B) employ automated or algorithmic systems in a manner consistent with any requirements for using merit systems personnel in public-benefits programs;

(C) identify instances in which reliance on automated or algorithmic systems would require notification by the State, local, Tribal, or territorial government to the Secretary;

(D) identify instances when applicants and participants can appeal benefit determinations to a human reviewer for reconsideration and can receive other customer support from a human being;

(E) enable auditing and, if necessary, remediation of the logic used to arrive at an individual decision or determination to facilitate the evaluation of appeals; and

(F) enable the analysis of whether algorithmic systems in use by benefit programs achieve equitable outcomes.

7.3. Strengthening AI and Civil Rights in the Broader Economy. (a) Within 365 days of the date of this order, to prevent unlawful discrimination from AI used for hiring, the Secretary of Labor shall publish guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems.

(b) To address discrimination and biases against protected groups in housing markets and consumer financial markets, the Director of the Federal Housing Finance Agency and the Director of the Consumer Financial Protection Bureau are encouraged to consider using their authorities, as they deem appropriate, to require their respective regulated entities, where possible, to use appropriate methodologies including AI tools to ensure compliance with Federal law and:

(i) evaluate their underwriting models for bias or disparities affecting protected groups; and

(ii) evaluate automated collateral-valuation and appraisal processes in ways that minimize bias.

(c) Within 180 days of the date of this order, to combat unlawful discrimination enabled by automated or algorithmic tools used to make decisions about access to housing and in other real estate-related transactions, the Secretary of Housing and Urban Development shall, and the Director of the Consumer Financial Protection Bureau is encouraged to, issue additional guidance:

(i) addressing the use of tenant screening systems in ways that may violate the Fair Housing Act (Public Law 90-284), the Fair Credit Reporting Act (Public Law 91-508), or other relevant Federal laws, including how the use of data, such as criminal records, eviction records, and credit information, can lead to discriminatory outcomes in violation of Federal law; and

(ii) addressing how the Fair Housing Act, the Consumer Financial Protection Act of 2010 (title X of Public Law 111-203), or the Equal Credit Opportunity Act (Public Law 93-495) apply to the advertising of housing, credit, and other real estate-related transactions through digital platforms, including those that use algorithms to facilitate advertising delivery, as well as on best practices to avoid violations of Federal law.

(d) To help ensure that people with disabilities benefit from AI's promise while being protected from its risks, including unequal treatment from the use of biometric data like gaze direction, eye tracking, gait analysis, and hand motions, the Architectural and Transportation Barriers Compliance Board is encouraged, as it deems appropriate, to solicit public participation and conduct community engagement; to issue technical assistance and recommendations on the risks and benefits of AI in using biometric data as an input; and to provide people with disabilities access to information and communication technology and transportation services.

Sec. 8. Protecting Consumers, Patients, Passengers, and Students. (a) Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models.

(b) To help ensure the safe, responsible deployment and use of AI in the healthcare, public-health, and human-services sectors:

(i) Within 90 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an HHS AI Task Force that shall, within 365 days of its creation, develop a strategic plan that includes policies and frameworks — possibly including regulatory action, as appropriate — on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health), and identify appropriate guidance and
resources to promote that deployment, including in the following areas:

(A) development, maintenance, and use of predictive and generative AI-enabled technologies in healthcare delivery and financing — including quality measurement, performance improvement, program integrity, benefits administration, and patient experience — taking into account considerations such as appropriate human oversight of the application of AI-generated output;

(B) long-term safety and real-world performance monitoring of AI-enabled technologies in the health and human services sector, including clinically relevant or significant modifications and performance across population groups, with a means to communicate product updates to regulators, developers, and users;

(C) incorporation of equity principles in AI-enabled technologies used in the health and human services sector, using disaggregated data on affected populations and representative population data sets when developing new models, monitoring algorithmic performance against discrimination and bias in existing models, and helping to identify and mitigate discrimination and bias in current systems;

(D) incorporation of safety, privacy, and security standards into the software-development lifecycle for protection of personally identifiable information, including measures to address AI-enhanced cybersecurity threats in the health and human services sector;

(E) development, maintenance, and availability of documentation to help users determine appropriate and safe uses of AI in local settings in the health and human services sector;

(F) work to be done with State, local, Tribal, and territorial health and human services agencies to advance positive use cases and best practices for use of AI in local settings; and

(G) identification of uses of AI to promote workplace efficiency and satisfaction in the health and human services sector, including reducing administrative burdens.

(ii) Within 180 days of the date of this order, the Secretary of HHS shall direct HHS components, as the Secretary of HHS deems appropriate, to develop a strategy, in consultation with relevant agencies, to determine whether AI-enabled technologies in the health and human services sector maintain appropriate levels of quality, including, as appropriate, in the areas described in subsection (b)(i) of this section. This work shall include the development of AI assurance policy — to evaluate important aspects of the performance of AI-enabled healthcare tools — and infrastructure needs for enabling pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data.

(iii) Within 180 days of the date of this order, the Secretary of HHS shall, in consultation with relevant agencies as the Secretary of HHS deems appropriate, consider appropriate actions to advance the prompt understanding of, and compliance with, Federal nondiscrimination laws by health and human services providers that receive Federal financial assistance, as well as how those laws relate to AI. Such actions may include:

(A) convening and providing technical assistance to health and human services providers and payers about their obligations under Federal nondiscrimination and privacy laws as they relate to AI and the potential consequences of noncompliance; and

(B) issuing guidance, or taking other action as appropriate, in response to any complaints or other reports of noncompliance with Federal nondiscrimination and privacy laws as they relate to AI.

(iv) Within 365 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an AI safety program that, in partnership with voluntary federally listed Patient Safety Organizations:

(A) establishes a common framework for approaches to identifying and capturing clinical errors resulting from AI deployed in healthcare settings as well as specifications for a central tracking repository for associated incidents that cause harm, including through bias or discrimination, to patients, caregivers, or other parties;

(B) analyzes captured data and generated evidence to develop, wherever appropriate, recommendations, best practices, or other informal guidelines aimed at avoiding these harms; and

(C) disseminates those recommendations, best practices, or other informal guidance to appropriate stakeholders, including healthcare providers.

(v) Within 365 days of the date of this order, the Secretary of HHS shall develop a strategy for regulating the use of AI or AI-enabled tools in drug-development processes. The strategy shall, at a minimum:

(A) define the objectives, goals, and high-level principles required for appropriate regulation throughout each phase of drug development;

(B) identify areas where future rulemaking, guidance, or additional statutory authority may be necessary to implement such a regulatory system;

(C) identify the existing budget, resources, personnel, and potential for new public/private partnerships necessary for such a regulatory system; and

(D) consider risks identified by the actions undertaken to implement section 4 of this order.

(c) To promote the safe and responsible development and use of AI in the transportation sector, in consultation with relevant agencies:

(i) Within 30 days of the date of this order, the Secretary of Transportation shall direct the Nontraditional and Emerging Transportation Technology (NETT) Council to assess the need for information, technical assistance, and guidance regarding the use of AI in transportation. The Secretary of Transportation shall further direct the NETT Council, as part of any such efforts, to:

(A) support existing and future initiatives to pilot transportation-related applications of AI, as they align with policy priorities articulated in the Department of Transportation's (DOT) Innovation Principles, including, as appropriate, through technical assistance and connecting stakeholders;

(B) evaluate the outcomes of such pilot programs in order to assess when DOT, or other Federal or State agencies, have sufficient information to take regulatory actions, as appropriate, and recommend appropriate actions when that information is available; and

(C) establish a new DOT Cross-Modal Executive Working Group, which will consist of members from different divisions of DOT and coordinate applicable work among these divisions, to solicit and use relevant input from appropriate stakeholders.

(ii) Within 90 days of the date of this order, the Secretary of Transportation shall direct appropriate Federal Advisory Committees of the DOT to provide advice on the safe and responsible use of AI in transportation. The committees shall include the Advanced Aviation

Advisory Committee, the Transforming Transportation Advisory Committee, and the Intelligent Transportation Systems Program Advisory Committee.

(iii) Within 180 days of the date of this order, the Secretary of Transportation shall direct the Advanced Research Projects Agency-Infrastructure (ARPA-I) to explore the transportation-related opportunities and challenges of AI — including regarding software-defined AI enhancements impacting autonomous mobility ecosystems. The Secretary of Transportation shall further encourage ARPA-I to prioritize the allocation of grants to those opportunities, as appropriate. The work tasked to ARPA-I shall include soliciting input on these topics through a public consultation process, such as an RFI.

(d) To help ensure the responsible development and deployment of AI in the education sector, the Secretary of Education shall, within 365 days of the date of this order, develop resources, policies, and guidance regarding AI. These resources shall address safe, responsible, and nondiscriminatory uses of AI in education, including the impact AI systems have on vulnerable and underserved communities, and shall be developed in consultation with stakeholders as appropriate. They shall also include the development of an "AI toolkit" for education leaders implementing recommendations from the Department of Education's AI and the Future of Teaching and Learning report, including appropriate human review of AI decisions, designing AI systems to enhance trust and safety and align with privacy-related laws and regulations in the educational context, and developing education-specific guardrails.

(e) The Federal Communications Commission is encouraged to consider actions related to how AI will affect communications networks and consumers, including by:

(i) examining the potential for AI to improve spectrum management, increase the efficiency of non-Federal spectrum usage, and expand opportunities for the sharing of non-Federal spectrum;

(ii) coordinating with the National Telecommunications and Information Administration to create opportunities for sharing spectrum between Federal and non-Federal spectrum operations;

(iii) providing support for efforts to improve network security, resiliency, and interoperability using next-generation technologies that incorporate AI, including self-healing networks, 6G, and Open RAN; and

(iv) encouraging, including through rulemaking, efforts to combat unwanted robocalls and robotexts that are facilitated or exacerbated by AI and to deploy AI technologies that better serve consumers by blocking unwanted robocalls and robotexts.

Sec. 9. Protecting Privacy. (a) To mitigate privacy risks potentially exacerbated by AI — including by AI's facilitation of the collection or use of information about individuals, or the making of inferences about individuals — the Director of OMB shall:

(i) evaluate and take steps to identify commercially available information (CAI) procured by agencies, particularly CAI that contains personally identifiable information and including CAI procured from data brokers and CAI procured and processed indirectly through vendors, in appropriate agency inventory and reporting processes (other than when it is used for the purposes of national security);

(ii) evaluate, in consultation with the Federal Privacy Council and the Interagency Council on Statistical Policy, agency standards and procedures associated with the collection, processing, maintenance, use, sharing, dissemination, and disposition of CAI that contains personally identifiable information (other than when it is used for the purposes of national security) to inform potential guidance to agencies on ways to mitigate privacy and confidentiality risks from agencies' activities related to CAI;

(iii) within 180 days of the date of this order, in consultation with the Attorney General, the Assistant to the President for Economic Policy, and the Director of OSTP, issue an RFI to inform potential revisions to guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002 (Public Law 107-347). The RFI shall seek feedback regarding how privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI; and

(iv) take such steps as are necessary and appropriate, consistent with applicable law, to support and advance the near-term actions and long-term strategy identified through the RFI process, including issuing new or updated guidance or RFIs or consulting other agencies or the Federal Privacy Council.

(b) Within 365 days of the date of this order, to better enable agencies to use PETs to safeguard Americans' privacy from the potential threats exacerbated by AI, the Secretary of Commerce, acting through the Director of NIST, shall create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI. The guidelines shall, at a minimum, describe the significant factors that bear on differential-privacy safeguards and common risks to realizing differential privacy in practice.

(c) To advance research, development, and implementation related to PETs:

(i) Within 120 days of the date of this order, the Director of NSF, in collaboration with the Secretary of Energy, shall fund the creation of a Research Coordination Network (RCN) dedicated to advancing privacy research and, in particular, the development, deployment, and scaling of PETs. The RCN shall serve to enable privacy researchers to share information, coordinate and collaborate in research, and develop standards for the privacy-research community.

(ii) Within 240 days of the date of this order, the Director of NSF shall engage with agencies to identify ongoing work and potential opportunities to incorporate PETs into their operations. The Director of NSF shall, where feasible and appropriate, prioritize research — including efforts to translate research discoveries into practical applications — that encourage the adoption of leading-edge PETs solutions for agencies' use, including through research engagement through the RCN described in subsection (c)(i) of this section.

(iii) The Director of NSF shall use the results of the United States-United Kingdom PETs Prize Challenge to inform the approaches taken, and opportunities identified, for PETs research and adoption.

Sec. 10. Advancing Federal Government Use of AI.

10.1. Providing Guidance for AI Management. (a) To coordinate the use of AI across the Federal Government, within 60 days of the date of this order and on an ongoing basis as necessary, the Director of OMB shall convene and chair an interagency council to coordinate the development and use of AI in agencies' programs and operations, other than the use of AI in national security systems. The Director of OSTP shall serve as Vice Chair for the interagency council. The interagency council's membership shall include, at minimum, the heads of the agencies identified in 31 U.S.C. 901(b), the Director of National Intelligence, and other agencies as identified by the Chair. Until agencies designate their permanent Chief AI Officers consistent with the guidance described in subsection 10.1(b) of this section, they shall be represented on the interagency council by an appropriate official at the Assistant Secretary level or equivalent, as determined by the head of each agency.

(b) To provide guidance on Federal Government use of AI, within 150 days of the date of this order and updated periodically thereafter, the Director of OMB, in coordination with the Director of OSTP, and in consultation with the interagency council established in subsection 10.1(a) of this section, shall issue guidance to agencies to strengthen the effective and appropriate use of AI, advance AI innovation, and manage risks from AI in the Federal Government. The Director of OMB's guidance shall specify, to the extent appropriate and consistent with applicable law:

(i) the requirement to designate at each agency within 60 days of the issuance of the guidance a Chief Artificial Intelligence Officer who shall hold primary responsibility in their agency, in coordination with other responsible officials, for coordinating their agency's use of AI, promoting AI innovation in their agency, managing risks from their agency's use of AI, and carrying out the responsibilities described in section 8(c) of Executive Order 13960 of December 3, 2020 (Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government), and section 4(b) of Executive Order 14091;

(ii) the Chief Artificial Intelligence Officers' roles, responsibilities, seniority, position, and reporting structures;

(iii) for the agencies identified in 31 U.S.C. 901(b), the creation of internal Artificial Intelligence Governance Boards, or other appropriate mechanisms, at each agency within 60 days of the issuance of the guidance to coordinate and govern AI issues through relevant senior leaders from across the agency;

(iv) required minimum risk-management practices for Government uses of AI that impact people's rights or safety, including, where appropriate, the following practices derived from OSTP's Blueprint for an AI Bill of Rights and the NIST AI Risk Management Framework: conducting public consultation; assessing data quality; assessing and mitigating disparate impacts and algorithmic discrimination; providing notice of the use of AI; continuously monitoring and evaluating deployed AI; and granting human consideration and remedies for adverse decisions made using AI;

(v) specific Federal Government uses of AI that are presumed by default to impact rights or safety;

(vi) recommendations to agencies to reduce barriers to the responsible use of AI, including barriers related to information technology infrastructure, data, workforce, budgetary restrictions, and cybersecurity processes;

(vii) requirements that agencies identified in 31 U.S.C. 901(b) develop AI strategies and pursue high-impact AI use cases;

(viii) in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other appropriate agencies as determined by the Director of OMB, recommendations to agencies regarding:

(A) external testing for AI, including AI red-teaming for generative AI, to be developed in coordination with the Cybersecurity and Infrastructure Security Agency;

(B) testing and safeguards against discriminatory, misleading, inflammatory, unsafe, or deceptive outputs, as well as against producing child sexual abuse material and against producing non-consensual intimate imagery of real individuals (including intimate digital depictions of the body or body parts of an identifiable individual), for generative AI;

(C) reasonable steps to watermark or otherwise label output from generative AI;

(D) application of the mandatory minimum risk-management practices defined under subsection 10.1(b)(iv) of this section to procured AI;

(E) independent evaluation of vendors' claims concerning both the effectiveness and risk mitigation of their AI offerings;

(F) documentation and oversight of procured AI;

(G) maximizing the value to agencies when relying on contractors to use and enrich Federal Government data for the purposes of AI development and operation;

(H) provision of incentives for the continuous improvement of procured AI; and

(I) training on AI in accordance with the principles set out in this order and in other references related to AI listed herein; and

(ix) requirements for public reporting on compliance with this guidance.

(c) To track agencies' AI progress, within 60 days of the issuance of the guidance established in subsection 10.1(b) of this section and updated periodically thereafter, the Director of OMB shall develop a method for agencies to track and assess their ability to adopt AI into their programs and operations, manage its risks, and comply with Federal policy on AI. This method should draw on existing related efforts as appropriate and should address, as appropriate and consistent with applicable law, the practices, processes, and capabilities necessary for responsible AI adoption, training, and governance across, at a minimum, the areas of information technology infrastructure, data, workforce, leadership, and risk management.

(d) To assist agencies in implementing the guidance to be established in subsection 10.1(b) of this section:

(i) within 90 days of the issuance of the guidance, the Secretary of Commerce, acting through the Director of NIST, and in coordination with the Director of OMB and the Director of OSTP, shall develop guidelines, tools, and practices to support implementation of the minimum risk-management practices described in subsection 10.1(b)(iv) of this section; and

(ii) within 180 days of the issuance of the guidance, the Director of OMB shall develop an initial means to ensure that agency contracts for the acquisition of AI systems and services align with the guidance described in subsection 10.1(b) of this section and advance the other aims identified in section 7224(d)(1) of the Advancing American AI Act (Public Law 117-263, div. G, title LXXII, subtitle B).

(e) To improve transparency for agencies' use of AI, the Director of OMB shall, on an annual basis, issue instructions to agencies for the collection, reporting, and publication of agency AI use cases, pursuant to section 7225(a) of the Advancing American AI Act. Through these instructions, the Director shall, as appropriate, expand agencies' reporting on how they are managing risks from their AI use cases and update or replace the guidance originally established in section 5 of Executive Order 13960.

(f) To advance the responsible and secure use of generative AI in the Federal Government:

(i) As generative AI products become widely available and common in online platforms, agencies are discouraged from imposing broad general bans or blocks on agency use of generative AI. Agencies should instead limit access, as necessary, to specific generative AI services based on specific risk assessments; establish guidelines and limitations on the appropriate use of generative AI; and, with appropriate safeguards in place, provide their personnel and programs with access to secure and reliable generative AI capabilities, at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans' rights. To protect Federal Government information, agencies are also encouraged to employ risk-management practices, such as training their staff on proper use, protection, dissemination, and disposition of Federal information; negotiating appropriate terms of service with vendors; implementing measures designed to ensure compliance with record-keeping, cybersecurity, confidentiality, privacy, and data protection requirements; and deploying other measures to prevent misuse of Federal Government information in generative AI.

(ii) Within 90 days of the date of this order, the Administrator of General Services, in coordination with the Director of OMB, and in consultation with the Federal Secure Cloud Advisory Committee and other relevant agencies as the Administrator of General Services may deem appropriate, shall develop and issue a framework for prioritizing critical and emerging technologies offerings in the Federal Risk and Authorization Management Program authorization process, starting with generative AI offerings that have the primary purpose of providing large language model-based chat interfaces, code-generation and debugging tools, and associated application programming interfaces, as well as prompt-based image generators. This framework shall apply for no less than 2 years from the date of its issuance. Agency Chief Information Officers, Chief Information Security Officers, and authorizing officials are also encouraged to prioritize generative AI and other critical and emerging technologies in granting authorities for agency operation of information technology systems and any other applicable release or oversight processes, using continuous authorizations and approvals wherever feasible.

(iii) Within 180 days of the date of this order, the Director of the Office of Personnel Management (OPM), in coordination with the Director of OMB, shall develop guidance on the use of generative AI for work by the Federal workforce.

(g) Within 30 days of the date of this order, to increase agency investment in AI, the Technology Modernization Board shall consider, as it deems appropriate and consistent with applicable law, prioritizing funding for AI projects for the Technology Modernization Fund for a period of at least 1 year. Agencies are encouraged to submit to the Technology Modernization Fund project funding proposals that include AI — and particularly generative AI — in service of mission delivery.

(h) Within 180 days of the date of this order, to facilitate agencies' access to commercial AI capabilities, the Administrator of General Services, in coordination with the Director of OMB, and in collaboration with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, the Administrator of the National Aeronautics and Space Administration, and the head of any other agency identified by the Administrator of General Services, shall take steps consistent with applicable law to facilitate access to Federal Government-wide acquisition solutions for specified types of AI services and products, such as through the creation of a resource guide or other tools to assist the acquisition workforce. Specified types of AI capabilities shall include generative AI and specialized computing infrastructure.

(i) The initial means, instructions, and guidance issued pursuant to subsections 10.1(a)-(h) of this section shall not apply to AI when it is used as a component of a national security system, which shall be addressed by the proposed National Security Memorandum described in subsection 4.8 of this order.

10.2. Increasing AI Talent in Government. (a) Within 45 days of the date of this order, to plan a national surge in AI talent in the Federal Government, the Director of OSTP and the Director of OMB, in consultation with the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Assistant to the President and Domestic Policy Advisor, and the Assistant to the President and Director of the Gender Policy Council, shall identify priority mission areas for increased Federal Government AI talent, the types of talent that are highest priority to recruit and develop to ensure adequate implementation of this order and use of relevant enforcement and regulatory authorities to address AI risks, and accelerated hiring pathways.

(b) Within 45 days of the date of this order, to coordinate rapid advances in the capacity of the Federal AI workforce, the Assistant to the President and Deputy Chief of Staff for Policy, in coordination with the Director of OSTP and the Director of OMB, and in consultation with the National Cyber Director, shall convene an AI and Technology Talent Task Force, which shall include the Director of OPM, the Director of the General Services Administration's Technology Transformation Services, a representative from the Chief Human Capital Officers Council, the Assistant to the President for Presidential Personnel, members of appropriate agency technology talent programs, a representative of the Chief Data Officer Council, and a representative of the interagency council convened under subsection 10.1(a) of this section. The Task Force's purpose shall be to accelerate and track the hiring of AI and AI-enabling talent across the Federal Government, including through the following actions:

(i) within 180 days of the date of this order, tracking and reporting progress to the President on increasing AI capacity across the Federal Government, including submitting to the President a report and recommendations for further increasing capacity;

(ii) identifying and circulating best practices for agencies to attract, hire, retain, train, and empower AI talent, including diversity, inclusion, and accessibility best practices, as well as to plan and budget adequately for AI workforce needs;

(iii) coordinating, in consultation with the Director of OPM, the use of fellowship programs and agency technology-talent programs and human-capital teams to build hiring capabilities, execute hires, and place AI talent to fill staffing gaps; and

(iv) convening a cross-agency forum for ongoing collaboration between AI professionals to share best practices and improve retention.

(c) Within 45 days of the date of this order, to advance existing Federal technology talent programs, the United States Digital Service, Presidential Innovation Fellowship, United States Digital Corps, OPM, and technology talent programs at agencies, with support from the AI and Technology Talent Task Force described in subsection 10.2(b) of this section, as appropriate and permitted by law, shall develop and begin to implement plans to support the rapid recruitment of individuals as part of a Federal Government-wide AI talent surge to accelerate the placement of key AI and AI-enabling talent in high-priority areas and to advance agencies' data and technology strategies.

(d) To meet the critical hiring need for qualified personnel to execute the initiatives in this order, and to improve Federal hiring practices for AI talent, the Director of OPM, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, conduct an evidence-based review on the need for hiring and workplace flexibility, including Federal Government-wide direct-hire authority for AI and related data-science and technical roles, and, where the Director of OPM finds such authority is appropriate, grant it; this review shall include the following job series at all General Schedule (GS) levels: IT Specialist (2210), Computer Scientist (1550), Computer Engineer (0854), and Program Analyst (0343) focused on AI, and any subsequently developed job series derived from these job series;

(ii) within 60 days of the date of this order, consider authorizing the use of excepted service appointments under 5 C.F.R. 213.3102(i)(3) to address the need for hiring additional staff to implement directives of this order;

(iii) within 90 days of the date of this order, coordinate a pooled-hiring action informed by subject-matter experts and using skills-based assessments to support the recruitment of AI talent across agencies;

(iv) within 120 days of the date of this order, as appropriate and permitted by law, issue guidance for agency application of existing pay flexibilities or incentive pay programs for AI, AI-enabling, and other key technical positions to facilitate appropriate use of current pay incentives;

(v) within 180 days of the date of this order, establish guidance and policy on skills-based, Federal Government-wide hiring of AI, data, and technology talent in order to increase access to those with nontraditional academic backgrounds to Federal AI, data, and technology roles;

(vi) within 180 days of the date of this order, establish an interagency working group, staffed with both human-resources professionals and recruiting technical experts, to facilitate Federal Government-wide hiring of people with AI and other technical skills;

(vii) within 180 days of the date of this order, review existing Executive Core Qualifications (ECQs) for Senior Executive Service (SES) positions informed by data and AI literacy competencies and, within 365 days of the date of this order, implement new ECQs as appropriate in the SES assessment process;

(viii) within 180 days of the date of this order, complete a review of competencies for civil engineers (GS-0810 series) and, if applicable, other related occupations, and make recommendations for ensuring that adequate AI expertise and credentials in these occupations in the Federal Government reflect the increased use of AI in critical infrastructure; and

(ix) work with the Security, Suitability, and Credentialing Performance Accountability Council to assess mechanisms to streamline and accelerate personnel-vetting requirements, as appropriate, to support AI and fields related to other critical and emerging technologies.

(e) To expand the use of special authorities for AI hiring and retention, agencies shall use all appropriate hiring authorities, including Schedule A(r) excepted service hiring and direct-hire authority, as applicable and appropriate, to hire AI talent and AI-enabling talent rapidly. In addition to participating in OPM-led pooled hiring actions, agencies shall collaborate, where appropriate, on agency-led pooled hiring under the Competitive Service Act of 2015 (Public Law 114-137) and other shared hiring. Agencies shall also, where applicable, use existing incentives, pay-setting authorities, and other compensation flexibilities, similar to those used for cyber and information technology positions, for AI and data-science professionals, as well as plain-language job titles, to help recruit and retain these highly skilled professionals. Agencies shall ensure that AI and other related talent needs (such as technology governance and privacy) are reflected in strategic workforce planning and budget formulation.

(f) To facilitate the hiring of data scientists, the Chief Data Officer Council shall develop a position-description library for data scientists (job series 1560) and a hiring guide to support agencies in hiring data scientists.

(g) To help train the Federal workforce on AI issues, the head of each agency shall implement — or increase the availability and use of — AI training and familiarization programs for employees, managers, and leadership in technology as well as relevant policy, managerial, procurement, regulatory, ethical, governance, and legal fields. Such training programs should, for example, empower Federal employees, managers, and leaders to develop and maintain an operating knowledge of emerging AI technologies to assess opportunities to use these technologies to enhance the delivery of services to the public, and to mitigate risks associated with these technologies. Agencies that provide professional-development opportunities, grants, or funds for their staff should take appropriate steps to ensure that employees who do not serve in traditional technical roles, such as policy, managerial, procurement, or legal fields, are nonetheless eligible to receive funding for programs and courses that focus on AI, machine learning, data science, or other related subject areas.

(h) Within 180 days of the date of this order, to address gaps in AI talent for national defense, the Secretary of Defense shall submit a report to the President through the Assistant to the President for National Security Affairs that includes:

(i)   recommendations to address challenges in the Department of Defense's ability to hire certain noncitizens, including at the Science and Technology Reinvention Laboratories;

(ii) recommendations to clarify and streamline processes for accessing classified information for certain noncitizens through Limited Access Authorization at Department of Defense laboratories;

(iii) recommendations for the appropriate use of enlistment authority under 10 U.S.C. 504(b)(2) for experts in AI and other critical and emerging technologies; and

(iv) recommendations for the Department of Defense and the Department of Homeland Security to work together to enhance the use of appropriate authorities for the retention of certain noncitizens of vital importance to national security by the Department of Defense and the Department of Homeland Security.

Sec. 11. Strengthening American Leadership Abroad. (a) To strengthen United States leadership of global efforts to unlock AI's potential and meet its challenges, the Secretary of State, in coordination with the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Director of OSTP, and the heads of other relevant agencies as appropriate, shall:

(i) lead efforts outside of military and intelligence areas to expand engagements with international allies and partners in relevant bilateral, multilateral, and multi-stakeholder fora to advance those allies' and partners' understanding of existing and planned AI-related guidance and policies of the United States, as well as to enhance international collaboration; and

(ii) lead efforts to establish a strong international framework for managing the risks and harnessing the benefits of AI, including by encouraging international allies and partners to support voluntary commitments similar to those that United States companies have made in pursuit of these objectives and coordinating the activities directed by subsections (b), (c), (d), and (e) of this section, and to develop common regulatory and other accountability principles for foreign nations, including to manage the risk that AI systems pose.

(b) To advance responsible global technical standards for AI development and use outside of military and intelligence areas, the Secretary of Commerce, in coordination with the Secretary of State and the heads of other relevant agencies as appropriate, shall lead preparations for a coordinated effort with key international allies and partners and with standards development organizations, to drive the development and implementation of AI-related consensus standards, cooperation and coordination, and information sharing. In particular, the Secretary of Commerce shall:

(i) within 270 days of the date of this order, establish a plan for global engagement on promoting and developing AI standards, with lines of effort that may include:

(A) AI nomenclature and terminology;

(B) best practices regarding data capture, processing, protection, privacy, confidentiality, handling, and analysis;

(C) trustworthiness, verification, and assurance of AI systems; and

(D) AI risk management;

(ii) within 180 days of the date the plan is established, submit a report to the President on priority actions taken pursuant to the plan; and

(iii) ensure that such efforts are guided by principles set out in the NIST AI Risk Management Framework and United States Government National Standards Strategy for Critical and Emerging Technology.

(c) Within 365 days of the date of this order, to promote safe, responsible, and rights-affirming development and deployment of AI abroad:

(i) The Secretary of State and the Administrator of the United States Agency for International Development, in coordination with the Secretary of Commerce, acting through the director of NIST, shall publish an AI in Global Development Playbook that incorporates the AI Risk Management Framework's principles, guidelines, and best practices into the social, technical, economic, governance, human rights, and security conditions of contexts beyond United States borders. As part of this work, the Secretary of State and the Administrator of the United States Agency for International

Development shall draw on lessons learned from programmatic uses of AI in global development.

(ii) The Secretary of State and the Administrator of the United States Agency for International Development, in collaboration with the Secretary of Energy and the Director of NSF, shall develop a Global AI Research Agenda to guide the objectives and implementation of AI-related research in contexts beyond United States borders. The Agenda shall:

(A) include principles, guidelines, priorities, and best practices aimed at ensuring the safe, responsible, beneficial, and sustainable global development and adoption of AI; and

(B) address AI's labor-market implications across international contexts, including by recommending risk mitigations.

(d) To address cross-border and global AI risks to critical infrastructure, the Secretary of Homeland Security, in coordination with the Secretary of State, and in consultation with the heads of other relevant agencies as the Secretary of Homeland Security deems appropriate, shall lead efforts with international allies and partners to enhance cooperation to prevent, respond to, and recover from potential critical infrastructure disruptions resulting from incorporation of AI into critical infrastructure systems or malicious use of AI.

(i) Within 270 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of State, shall develop a plan for multilateral engagements to encourage the adoption of the AI safety and security guidelines for use by critical infrastructure owners and operators developed in section 4.3(a) of this order.

(ii) Within 180 days of establishing the plan described in subsection (d)(i) of this section, the Secretary of Homeland Security shall submit a report to the President on priority actions to mitigate cross-border risks to critical United States infrastructure.

Sec. 12. Implementation. (a) There is established, within the Executive Office of the President, the White House Artificial Intelligence Council (White House AI Council). The function of the White House AI Council is to coordinate the activities of agencies across the Federal Government to ensure the effective formulation, development, communication, industry engagement related to, and timely implementation of AI-related policies, including policies set forth in this order.

(b) The Assistant to the President and Deputy Chief of Staff for Policy shall serve as Chair of the White House AI Council.

(c) In addition to the Chair, the White House AI Council shall consist of the following members, or their designees:

(i) the Secretary of State;

(ii) the Secretary of the Treasury;

(iii) the Secretary of Defense;

(iv) the Attorney General;

(v) the Secretary of Agriculture;

(vi) the Secretary of Commerce;

(vii) the Secretary of Labor;

(viii) the Secretary of HHS;

(ix) the Secretary of Housing and Urban Development;

(x) the Secretary of Transportation;

(xi) the Secretary of Energy;

(xii) the Secretary of Education;

(xiii) the Secretary of Veterans Affairs;

(xiv) the Secretary of Homeland Security;

(xv) the Administrator of the Small Business Administration;

(xvi) the Administrator of the United States Agency for International Development;

(xvii) the Director of National Intelligence;

(xviii) the Director of NSF;

(xix) the Director of OMB;

(xx) the Director of OSTP;

(xxi) the Assistant to the President for National Security Affairs;

(xxii) the Assistant to the President for Economic Policy;

(xxiii) the Assistant to the President and Domestic Policy Advisor;

(xxiv) the Assistant to the President and Chief of Staff to the Vice President;

(xxv) the Assistant to the President and Director of the Gender Policy Council;

(xxvi) the Chairman of the Council of Economic Advisers;

(xxvii) the National Cyber Director;

(xxviii) the Chairman of the Joint Chiefs of Staff; and

(xxix) the heads of such other agencies, independent regulatory agencies, and executive offices as the Chair may from time to time designate or invite to participate.

(d) The Chair may create and coordinate subgroups consisting of White House AI Council members or their designees, as appropriate.

Sec. 13. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,
October 30, 2023.

ALERT

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Release Date: November 28, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES </topics/cybersecurity-best-practices>

CISA is responding to active exploitation <https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal> of Unitronics programmable logic controllers (PLCs) used in the Water and Wastewater Systems (WWS) Sector <https://www.cisa.gov/water>. Cyber threat actors are targeting PLCs associated with WWS facilities, including an identified Unitronics PLC, at a U.S. water facility. In response, the affected municipality's water authority immediately took the system offline and switched to manual operations—there is no known risk to the municipality's drinking water or water supply.

WWS Sector facilities use PLCs to control and monitor various stages and processes of water and wastewater treatment, including turning on and off pumps at a pump station to fill tanks and reservoirs, flow pacing chemicals to meet regulations, gathering compliance data for monthly regulation reports, and announcing critical alarms to operations.

Attempts to compromise WWS integrity via unauthorized access threaten the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities.

The cyber threat actors likely accessed the affected device—a Unitronics Vision Series PLC with a Human Machine Interface (HMI)—by exploiting cybersecurity weaknesses, including poor password security and exposure to the internet. To secure WWS facilities against this threat, CISA urges organizations to:

- Change all default passwords on PLCs and HMIs and use a strong password <https://www.cisa.gov/secure-our-world/require-strong-passwords>. Ensure the Unitronics PLC default password "1111" is not in use.
- Require multifactor authentication for all remote access to the OT network, including from the IT network and external networks.

- Disconnect the PLC from the open internet. If remote access is necessary, control network access to the PLC.
    - Implement a Firewall/VPN in front of the PLC to control network access to the remote PLC. A VPN or gateway device can enable multifactor authentication for remote access even if the PLC does not support multifactor authentication. Unitronics also has a secure cellular based longhaul transport device that is secure to their cloud services.
    - Use an allowlist of IPs for access.
- Back up the logic and configurations on any Unitronics PLCs to enable fast recovery. Become familiar with the process for factory resetting and deploying configurations to a device in the event of being hit by ransomware.
- If possible, utilize a TCP port that is different than the default port TCP 20256. Cyber actors are actively targeting TCP 20256 after identifying it through network probing as a port associated to Unitronics PLC. Once identified, they leverage scripts specific to PCOM/TCP to query and validate the system, allowing for further probing and connection. If available, use PCOM/TCP filters to parse out the packets.

- **Updated Dec. 19, 2023:**
  - Update PLC/HMI to the latest version provided by Unitronics <https://www.unitronicsplc.com/cyber_security_vision-samba/>.
  - See Unitronics Cybersecurity Advisory 2023-001 <https://downloads.unitronicsplc.com/sites/plc/technical_library/unitronics-cybersecurity-advisory-2023-001-cve-2023-6448.pdf> for more information.
  - See joint Cybersecurity Advisory, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a> (published Dec. 1, 2023) for additional technical information and mitigations.
  - See CISA's Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords </resources-tools/resources/secure-design-alert-how-manufacturers-can-protect-customers-eliminating-default-passwords>.

CISA and WWS Sector partners have developed numerous tools and resources that water utilities can use to increase their cybersecurity. Please visit:

- CISA: Water and Wastewater Cybersecurity <https://www.cisa.gov/water>
- EPA: Cybersecurity for the Water Sector <https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector>
- WaterISAC: Resource Center <https://www.waterisac.org/resources>
- American Water Works Association: Cybersecurity and Guidance <https://www.awwa.org/resources-tools/resource-topics/risk-resilience/cybersecurity-guidance>

Report

All organizations should report suspicious or criminal activity related to information found in this Alert by contacting CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870, or your local FBI field office <https://www.fbi.gov/contact-us/field-offices>.

Tags

Topics: Cybersecurity Best Practices </topics/cybersecurity-best-practices>

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Related Advisories

MAR 08, 2024 **ALERT**

Apple Released Security Updates for Multiple Products </news-events/alerts/2024/03/08/apple-released-security-updates-multiple-products>

MAR 07, 2024 **ALERT**

CISA Releases One Industrial Control Systems Advisory </news-events/alerts/2024/03/07/cisa-releases-one-industrial-control-systems-advisory>

MAR 07, 2024 **ALERT**

Apple Releases Security Updates for iOS and iPadOS </news-events/alerts/2024/03/07/apple-releases-security-updates-ios-and-ipados>

MAR 07, 2024 **ALERT**

CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices </news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

888-282-0870 central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>	Accessibility </accessibility>	Budget and Performance <https://www.dhs.gov/performance-financial-reports>
DHS.gov <https://www.dhs.gov>	FOIA Requests <https://www.dhs.gov/foia>	No FEAR Act </cisa-no-fear-act-reporting>
Office of Inspector General <https://www.oig.dhs.gov/>	Privacy Policy </privacy-policy>	Subscribe
The White House <https://www.whitehouse.gov/>	USA.gov <https://www.usa.gov/>	Website Feedback </forms/feedback>

Planning Considerations for Cyber Incidents

Guidance for Emergency Managers

November 2023

FEMA

This page intentionally left blank.

Table of Contents

Introduction and Overview

1. Purpose

Emergency management personnel play a central role in preparing for and responding to cyber incidents in their jurisdictions.[1] Although emergency managers are not expected to be technical experts on cyber incidents, they do need to understand and prepare for the potential impacts of a cyber incident on their communities as well as on their emergency operations. Knowing whom to engage when a cyber incident occurs and having plans in place to effectively address an incident's impacts is central to the role of emergency managers, regardless of hazard type.

Developed by the Federal Emergency Management Agency (FEMA) in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), this guide is intended to help state, local, tribal, and territorial (SLTT) emergency management personnel collaboratively prepare for a cyber incident and support the development of a cyber incident response plan or annex. While focused on the roles and responsibilities that emergency managers in government may have, emergency managers in academia, nonprofits, or the private sector may also find the concepts helpful, especially if they serve on a jurisdiction's planning team.

1.1. Background

Nearly all aspects of society heavily rely on networked technologies. From phones and communications systems to home appliances and security systems, to transportation systems, medical systems, and utility services, nearly all aspects of society rely on networked technologies to communicate and operate. While increased interconnectedness provides better and more efficient services in many ways, the increasing reliance on technology and cyber connections may lead to cyber incidents with far-reaching and devastating impacts. An interruption in one organization or system, whether from a natural hazard, human error, equipment failure, or malicious attack, may have widespread impacts across a network. In the worst cases, this puts lives at risk and causes significant economic challenges. For these reasons, it is increasingly important that organizations and jurisdictions have a cybersecurity program in place to protect against disruptions and a cyber incident response plan in place to enable quick, effective resolutions when an incident occurs.

1.2. Cybersecurity and Cyber Incident Response

It is important to understand the difference and relationship between cybersecurity and cyber incident response. "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and

[1] CISA leads the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure. CISA also coordinates the execution of national cyber defense, leads asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners. For more information, visit CISA.gov/about-cisa.

availability of information."[2] The goal of cybersecurity is to stop or minimize disruptions. A cybersecurity program is designed to both understand and address cyber risks across an enterprise and is composed of people, processes, and technologies that monitor, detect and, ideally, prevent incidents on an ongoing basis. However, even with the best cybersecurity program in place, cyber incidents are always a risk. Therefore, it is important to have a cyber incident response plan or annex that enables organizations to act quickly. An effective and efficient response helps to mitigate impacts and return functional services as soon as possible. Much of cyber incident response planning occurs before an incident occurs and in conjunction with a cybersecurity program.

Although a fully mature cybersecurity program includes cyber incident response planning, effective planning for cyber incidents requires specific areas of focus. This guide provides considerations for cyber incident response planning, in line with the six-step planning process outlined in FEMA's Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans. It does not provide guidance for establishing a cybersecurity program or its protocols. There are many useful resources available to help organizations and jurisdictions set up and implement a cybersecurity program. Several key resources are highlighted below.

Resources for Building or Strengthening a Cybersecurity Program

- Cybersecurity Performance Goals: Provide baseline information technology (IT) and operational technology (OT) security practices that can improve resilience against, and meaningfully reduce the likelihood and impact of, known cyber risks and common tactics, techniques, and procedures (TTPs).
- Cyber Security Evaluation Tool (CSET): Provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET includes the Cybersecurity Performance Goals Assessment, which organizations can use to evaluate their cybersecurity posture and drive investments towards meaningfully reducing the likelihood and impact of known risks and adversary techniques.
- National Institute of Standards and Technologies (NIST) Cybersecurity Framework: Provides strategic guidance to help build and execute a cybersecurity program. The framework helps organizations assess cyber risks and set plans for improving or maintaining their security posture.
- CISA Emergency Services Sector Cybersecurity Framework Implementation Guidance: Provides foundational guidance for how emergency services sector organizations may enhance their cybersecurity using the NIST Cybersecurity Framework.

In addition, understanding and managing cybersecurity risks are key to developing a strong program. The following resources can help organizations prioritize the most important activities:

[2] CISA, 2019, Security Tip (ST04-001), What is Cybersecurity?

- CISA Vulnerability Scanning: Provides automated vulnerability scans and delivers a weekly report, which helps secure internet-facing systems from weak configurations and known vulnerabilities.
- CISA Known Exploited Vulnerability (KEV) catalog: Authoritative source of vulnerabilities that have been exploited. Can be use by organizations to prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.
- CISA Emergency Services Sector Cybersecurity Initiative: Provides resources to help those in the emergency services sector better understand and manage cyber risks.
- CISA Cyber Essentials Starter Kit: Provides guidance for leaders of small businesses and small and local government agencies to help them start implementing organizational cybersecurity practices.
- CISA Free Cybersecurity Services and Tools: Identifies free cybersecurity tools and services to help organizations further advance their security capabilities.
- State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) Cyber Resource Compendium: Identifies some of the major references that may help build or strengthen an organization's cybersecurity program.
- Nationwide Cybersecurity Review (NCSR): Provides a no-cost, anonymous, annual self-assessment mechanism designed to measure gaps and capabilities of SLTTs' cybersecurity programs.

1.2.1. INTRODUCTION TO CYBER INCIDENT RESPONSE PLANNING

Cyber incidents, like other disruptive events, may have long-term unforeseen, cascading, and far-reaching consequences. The impacts may cause immediate consequences to a service or system, or indirect and cascading effects. Potential impacts are further complicated as cyber incidents may result from a variety of causes, such as a malicious attack, a natural disaster, human error, or equipment failure, each requiring distinct actions to resolve the situation. It may not be immediately known whether the root cause is cyber related. Emergency managers may be well into addressing the consequences of the event before realizing it is a cyber incident. For these reasons, cyber incident planning and response necessitate collaboration among emergency management, cyber professionals, law enforcement, private industry, and other key stakeholders.

Although incident response plans vary from organization to organization, their purpose is consistent: to enable effective and efficient response to a cyber incident, mitigate its impacts, and return services back to normal quickly. Having an effective cyber incident response plan in place before an incident occurs reduces the amount of time that organizations or jurisdictions spend determining who to contact, what to do, and defining ownership and responsibilities during the incident.

Incident response plans identify response team members and their backups, how to contact team members when an event is reported, and the roles of each team member. The plan outlines the steps taken at each stage of the process and designates the team member(s) responsible for each step, as well as the team member charged with overall responsibility for the response. Cyber incidents create significant ambiguity, so it is important for planners to ensure that the plan developed is flexible and adapts to changing circumstances. More information on the planning process is provided in Appendix A and further detailed in CPG 101: Developing and Maintain Emergency Operations Plans.

Specific to cyber planning, there are different cyber incident response approaches that jurisdictions may leverage when developing a cyber incident response plan. The National Institute of Standards and Technologies (NIST)'s approach is one of the most respected. NIST's Computer Security Incident Handling Guide "assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively."

NIST's approach applies a four-phase incident response lifecycle, shown in Figure 1 and listed below.[3]

1. **Preparation:** Preparation is essential to both preventing and responding to a disruptive cyber event. In preparing for a cyber incident, NIST suggests implementing a series of tools ahead of time. This preparation provides the community with a framework to analyze, isolate, and respond to an incident. Development of a clearly articulated cyber incident response plan with established points of contact, before an incident occurs, is important to this preparation phase.
2. **Detection and Analysis:** The second phase is determining an incident has occurred, its severity, and its type.
3. **Containment, Eradication and Recovery:** The third phase focuses on addressing the identified incident. It includes containment—preventing the spread of the incident and limiting its impact, eradication—removing the cause of the incident, and recovery—restoring normal operations and recovering any data that may have been lost or damaged. During this phase, the incident response team often cycles back to detection and analysis to ensure all elements of the incident have been identified.
4. **Post-Incident Activity:** This phase focuses on identifying lessons learned and opportunities for improvement. By evaluating the response process and outcome, organizations can identify best practices and make necessary changes to prevent similar incidents from occurring in the future. They can also identify areas for improvement in incident response planning, communication, and overall incident management.

[3] NIST, 2012, *Computer Security Incident Handling Guide*, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

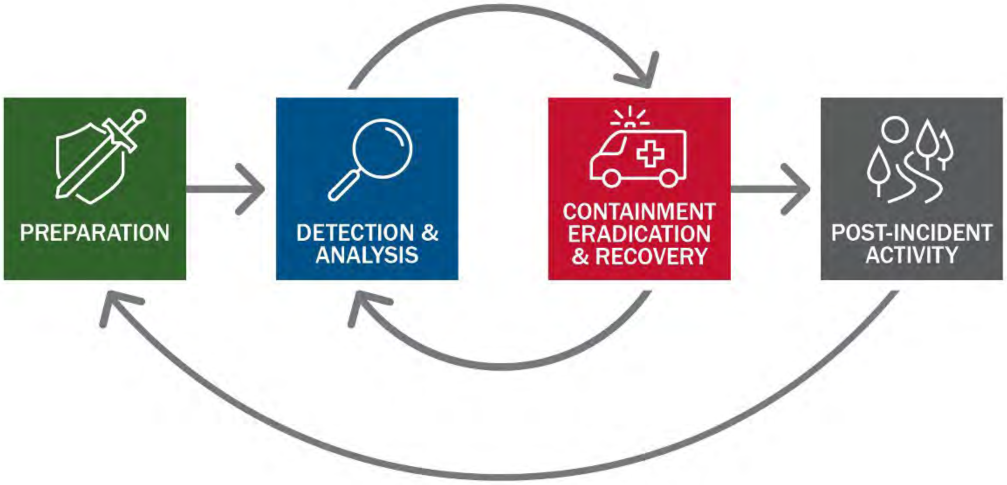


Figure 1: NIST Incident Response Lifecycle

Development of the incident response plan falls into the Preparation phase of the incident response lifecycle and will set the framework for executing the remaining phases when needed. Phases 2, 3 and 4 of the NIST incident response lifecycle are highly technical and require extensive cyber expertise. For this reason, it is essential that development of the cyber incident response plan is a collaborative effort among emergency management, cyber professionals, law enforcement, private industry, and other key stakeholders.

1.2.2. LEGAL CONSIDERATIONS

Emergency managers should consult with their legal advisors as they prepare for and respond to cyber incidents. Some jurisdictions already have specific laws or ordinances pertaining to cybersecurity and data protection, such as safeguards for personally identifiable data or cyber incident reporting. Although it mentions legal considerations, this document does not constitute or provide compliance or legal advice. This document is intended to be general guidance for a variety of factual circumstances, so readers should confer with their respective advisors to obtain advice based on their individual circumstances and applicable legal requirements.

2. Types of Cyber Incidents

A key step in planning for cyber incident response is identifying the types of cyber incidents that the jurisdiction may face. While it is not feasible to comprehensively identify all the specific cyber incidents that could impact an organization, it is important for emergency managers to have a general understanding of the common types of cyber incidents, along with the types of systems incidents may impact. Incidents may impact the OT/industrial control systems (ICS) that operate, control, and monitor industrial processes throughout U.S. infrastructure along with the associated IT systems. Owners and operators who understand cyber actors' TTPs can use that knowledge to prioritize hardening actions. Partnerships with other key personnel and subject matter experts help identify the types of incidents most likely to occur among these varying types of systems in the jurisdiction and their immediate and cascading impacts. This foundational understanding of the common types of cyber incidents also helps with the development of incident scenarios that are useful to the planning process.

This section provides a general overview of key cyber concepts and incident types. It first describes the primary types of cyber assets and the role they may play in cyber incidents, then reviews the common causes of cyber disruptions. The content in this section is not intended to be all-encompassing. Please see the glossary for additional cyber terms and definitions.

Cyber Assets and Systems[4]

Assets are items of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation).

Systems are a combination of interacting elements organized to achieve one or more stated purposes. Interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities.

Operational Technology (OT)/Industrial Control Systems (ICS) include a broad range of programmable systems and devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring or control of devices, processes, and events. ICS are an example of OT that control critical infrastructures.

2.1. Overview of Cyber Assets and Incident Types

Cyber assets include hardware, software, and networks. Hardware performs the physical functions, software directs and controls the hardware, and a network is a connection of computers enabling them to communicate and share information. Cyber assets range from systems with local networks to assets with internet access including smart phones, security systems, building management systems, heating and air conditioning systems, phone systems, smart home devices, vehicle control systems, and more. Identifying critical services in the jurisdiction and understanding how those services depend upon different types of cyber assets allows jurisdictions to assess how different types of incidents might affect their key functions. Impacts will often cascade, meaning that a particular impact on a specific system may be caused by an impact on an upstream system, or may cause further impact on a downstream system.

Below is an overview of three common cyber incident types. Although each is described independently, any of these incident types is likely to cause overlapping and cascading effects. The

[4] NIST, 2021, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

compromise of any hardware, software, or network is likely to result in the loss or degradation of services and may allow a malicious actor access to confidential information or system controls.

- **Hardware Destruction or Loss**: A jurisdiction's critical services often depend upon the hardware (e.g., computers, industrial control systems, storage devices, network infrastructure) that perform critical functions. This hardware may enable day-to-day community functions, such as controlling drinking water systems and water filtration, managing court processes, providing payment systems for municipal services, and controlling traffic safety systems. It also may support critical emergency services, such as 911 services and radio transmitters used to communicate among emergency personnel. The infrastructure that provides these services may be overlapping. Hardware damage may result in the loss of computer and network communication services as well as the loss of data and can disrupt critical services. Hardware destruction or loss can be caused by natural hazards including floods, fires, and tornados, as well as electricity surges resulting from natural phenomenon such as lightning or geomagnetic disturbances/storms. Damage can also be caused by malicious acts. The unusual loss of a controller can be a complex issue to investigate. Engineers may initially attribute the loss to equipment failure, but further examination may uncover that it was due to a malicious attack on the controller, where a threat actor has introduced malicious code or malware and caused a catastrophic failure of the controller. This can have potentially devastating consequences for the system, leading to extended downtime and disruption of operations. It is therefore essential to investigate any unusual losses of controllers and identify the cause to ensure the security of the system.

- **Network Unavailability, Compromise, Degradation, or Destruction**: Networks enable computers to communicate and share information. Most critical services rely on networks. Incidents affecting networks may occur because of both natural disasters and malicious attacks. Since many systems depend upon external organizations and are often provided by third parties, an incident affecting the jurisdiction may be the result of a third party's incident. The impact may vary from unreliable communication among computers to a complete loss of communication. Identifying how the jurisdiction uses networks helps the planning team to understand how the jurisdiction depends upon these systems and to evaluate the potential consequence of their loss.

- **Software Malfunction, Compromise, or Exploitation**: Incidents affecting software may cause the loss or compromise of critical functions. Most of these incidents are caused by human error or accidental misconfigurations. However, incidents affecting software may also result from malicious attacks. Malicious actors may steal confidential information, modify and violate the integrity of information, or deny access to information by encrypting it and demanding money (ransom) to decrypt it. Malicious actors may also exploit software to compromise the integrity of physical systems such as security cameras, water and wastewater treatment, dams, traffic signs and signals, streetlights, pipelines, and facility management, which are often controlled (or monitored) by computerized industrial control systems.

2.2. Overview of Incident Cause

In most cases, determining the cause of a cyber disruption requires extensive cyber expertise. It is often unclear at the beginning of an incident whether the effects are caused by a malicious actor or another source, and it may take days or months to determine. The information in this section is not intended to help identify the cause of a particular incident. Rather, it is intended to highlight the primary causes of incidents to help the planning team think through potential cyber incidents that may occur in their jurisdiction, whether the result of natural hazards, accidents, or intentional attacks.

2.2.1. NON-MALICIOUS INCIDENTS

Non-malicious cyber incidents happen for numerous reasons. NIST includes the following non-malicious causes when categorizing threat sources: human errors, structural failures of organization-controlled resources (e.g., hardware, software, environmental controls), and natural and human-caused disasters, which are accidents and failures beyond the control of the organization.[5]

- Human Error: Cyber incidents may be caused by accidental errors made by individuals while performing their regular responsibilities. For example, mistakes happen while performing administrative tasks, such as installing or configuring hardware and software or conducting maintenance of computers and networks. These unintentional errors cause incidents that disable, disrupt, or damage computers, networks, and information.

- Structural Failures: These incidents happen when hardware, software, or support systems, such as environmental controls (e.g., air conditioning), fail. Hardware and software often contain unknown flaws that appear unexpectedly. These flaws may cause incidents ranging from loss of services to the loss or corruption of important information. When computing or networking demands exceed the capacities of the cyber resources, the cyber services might stop operating, corrupt or lose important information, or create other problems.

- Natural Disasters: All types of cyber assets depend upon physical systems ranging from hardware for computers and networks to the infrastructure that manages operational environments. Natural disasters and accidents may damage or disrupt the operation of physical systems. Fires, floods, windstorms, and electrical disturbances often cause non-malicious cyber incidents. Loss of electrical power is another common cause. Uninterruptible power supplies handle short-term power problems, and alternative power generation systems such as diesel generators handle long-term losses, provided fuel is available.

[5] NIST, 2012, *Guide for Conducting Risk Assessments*, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

2.2.2. MALICIOUS INCIDENTS

Malicious actors attempt to compromise the availability, integrity, or confidentiality of computers, networks or information. As noted above, the specific cause of an incident will rarely be known while the event takes place. More often, it is discovered days or months later following a forensic examination of the impacted equipment or software.

- **Denial of Service (DoS)**: DoS attacks flood computers and networks with traffic that overloads a network and disrupts legitimate requests. Such traffic often originates from multiple locations to complicate attempts to block them and may serve to amplify the malicious traffic directed at the targeted computers. These are described as distributed denial-of-service (DDoS) attacks. By limiting access to websites used for business operations, malicious actors may cause a variety of issues, including financial losses or damage to the reputation of businesses. Similarly, malicious actors have used DDoS attacks to deny access to government websites.

- **Malware**: Malware is a broad term for any type of malicious software designed to harm or exploit a programmable device, service, or network. Malware appears in various forms and may perform a wide variety of malicious actions:

    - Ransomware uses encryption to deny access to information. Ransomware actors demand ransom to decrypt the information and may also threaten to publish the information unless the ransom is paid.

    - Spyware infects computers and collects information about user activity, such as usernames and passwords, payment information, information in emails, and other sensitive information that may enable threat actors to perform other malicious activity.

    - A trojan provides a backdoor gateway for malicious programs or threat actors to enter a system and steal valuable data without the user's knowledge or permission.

    - A worm replicates and spreads across devices within a network. As it spreads, it consumes bandwidth, overloading infected systems, and making them unreliable or unavailable.

A common delivery method for cyber intrusions is **Phishing**. Malicious actors use phishing attacks to steal sensitive information and potentially enable malicious access to a computer or system. Phishing is typically conducted through email or text messages (smishing) to trick people into clicking a link, downloading malicious software (malware) or revealing login credentials. If successful, phishing may infect the email recipient's computer. Spear phishing is a tactic that targets specific organizations or individuals with personalized messages that deceives the receiver into trusting the message. For more information about phishing, see CISA's guide on Phishing Guidance: Stopping the Attack Cycle at Phase One.

- **Third-Party Compromises and Supply Chain Attacks:** Malicious actors attack third-party vendors of software and services because other organizations rely upon and trust vendors and install their software to manage complex systems. Adversaries gain access to third-party vendor software to exploit the modified software once installed by the vendor's customers.

3. Assessing Cyber Risks to Inform Prioritization and Planning

Effective preparedness for cyber incidents requires that jurisdictions understand how essential services and infrastructure in the community, including emergency management services and infrastructure, rely on cyber systems and the potential cascading impacts of a disruption. This knowledge helps the jurisdiction's planning team determine response actions and resources that are needed in a cyber incident, as well as how to prioritize restoration efforts.

3.1. Engaging Service Owners and Operators

Owners and operators of critical services and their associated cyber systems play an important role in preparing for cyber incidents, including assessing cyber risks. The owners and operators provide the most detailed and accurate information regarding system dependencies and vulnerabilities and valuable guidance on assessing whether the service remains operational during and following an incident. Engaging owners and operators in assessing cyber risks and planning for cyber incidents also helps establish relationships with cyber staff and service providers. These relationships foster a shared understanding of vulnerabilities and impacts related to specific incident types and aid in the development of effective plans, policies, procedures, and protocols.

Engagement with owners and operators of critical services and cyber systems is essential to successful cyber incident response planning. However, some organizations may be reluctant to collaborate due to concerns such as sharing proprietary information, the risk of data leakage, and the potential for brand and financial damages in the event of an incident. Establishing a confidentiality agreement, Non-Disclosure Agreement (NDA), private-public partnership, or other legal agreement in consultation with appropriate legal advisors may reduce these concerns. FEMA's Building Private-Public Partnerships Guide[6] provides best practices for building and maintaining these partnerships.

[6] FEMA, 2021, *Building Private-Public Partnerships*, https://www.fema.gov/sites/default/files/documents/fema_building-private-public-partnerships.pdf.

Cyber Asset Owners and Operators

Asset owners are people or organizational entities, internally or externally, that have primary responsibility for the viability, productivity, and resilience of the asset.

Asset operators are people or organizational entities, internally or externally, who are responsible for satisfying the protection and sustainment requirements for the asset established by the asset owner. Asset operators include system/database administrators, industrial control system engineers, facility managers, IT support organizations, and contractors who host and manage data (e.g., cloud service provider).

3.2. Assessing Cyber Risks

Assessing cyber risks enables the jurisdiction to identify the most likely cyber disruptions with the most severe impact for their community. This aids the jurisdiction in identifying the response actions and resources needed in a cyber incident, as well as how to prioritize restoration efforts. Assessing cyber risks requires the following actions:

- Identifying the critical services for the community that rely on OT and IT, such as emergency services, water and wastewater systems, and communications.
- Identifying the dependencies of critical infrastructure, particularly those related to critical services, cyber assets, and services.
- Identifying the consequences of service loss or disruption, with special attention to the problems caused by cyber incidents.

Developing a critical services and dependencies inventory is a good way to identify, examine, and document this information. The inventory captures the critical services, infrastructure, assets, associated owners and operators, other key personnel, and the dependencies among systems. In addition to helping with this assessment and prioritization process, this inventory may also be included within the cyber incident response plan or annex for reference during an incident.

3.2.1. IDENTIFYING CRITICAL SERVICES

Identifying the jurisdiction’s critical services that rely on cyber systems is the first step in the assessment process. The planning team begins by identifying the known critical services and their owners and operators, then expands to identify other related services. This helps build the critical services and dependencies inventory. It also provides an opportunity to identify additional key stakeholders to include in the planning team (see Appendix A for information on the six-step planning process and for more guidance on forming the core and collaborative planning teams).

When identifying critical services, it may be beneficial to use community lifelines[7] as a starting point. Community lifelines are services that enable the continuous operation of critical government and business functions and are essential to human health and safety or economic security. They are the most fundamental services within a community that, when stabilized, enable all other aspects of society to function.

Continuity of Operations Planning

Continuity is the ability to provide uninterrupted critical services, essential functions, support, and other priority services while maintaining organizational viability, before, during, and after an event that disrupts normal operations.

It may be helpful to consider continuity planning best practices when establishing and updating cyber incident response plans. Cyber incidents may result in degraded communications, compromised systems, or inoperable facilities. It is crucial that jurisdictions' continuity assessments and plans include cyber considerations.

For more information on continuity planning, assessment tools and resources, visit: Continuity Resources and Technical Assistance at fema.gov.

3.2.2. IDENTIFYING SERVICE DEPENDENCIES

Identifying and understanding dependencies among systems and assets helps the planning team, and ultimately the incident response team, consider what may disrupt key services or other assets on which those services depend.[8] It also helps to identify the upstream or downstream implications. This process helps the planning team anticipate possible impacts to community lifelines, which may influence the prioritization of incident response decisions and actions.

Using the list of critical services and their owners and operators as a starting point, the planning team identifies service dependencies by:

- **Engaging with Service Owners and Operators:** The service owners and operators provide key information about the system to assist with building an understanding of the jurisdiction's dependencies.

- **Identifying and Engaging Other Stakeholders of Each Service:** Some services involve additional stakeholders beyond the system owner such as security professionals, third-party service providers, or a cyber incident response team (CIRT). Understanding all the stakeholders and their roles aids in identifying who is contacted when an incident occurs.

- **Identifying Support Contacts for All Vendors and Contracted Service Providers:** Not all services and systems are owned, serviced, or maintained by in-house staff. As a result, third-

[7] For more information on community lifelines, visit: https://www.fema.gov/emergency-managers/practitioners/lifelines.
[8] For an overview of dependencies, visit: https://www.cisa.gov/what-are-dependencies.

party or support contacts may need to be part of the planning effort. The planning team works with service owners to identify any support contracts and determine what these contracts may provide during an incident. For example, the internet service provider may help identify the type of attack and potentially block the attacker if requested.

As the planning team identifies and documents the dependencies in the critical services and dependency inventory, considerations include:

- **Upstream Dependencies:** These are products or services provided to a jurisdiction by an external organization that are necessary to support its operations and functions. Examples of upstream dependencies include:
  - Supply of electricity from an electric utility distribution substation;
  - Telephone communication services;
  - Access to the internet; and
  - External organizations, such as a vendor that maintains essential software systems.
- **Internal Dependencies:** These are the interactions among internal services, operations, functions, and information of the jurisdiction. Examples of internal dependencies include:
  - Information services, such as websites, depend upon database servers;
  - Operational control systems depend upon process measurement systems; and
  - Computer systems depend upon computer network equipment.
- **Downstream Dependencies:** These are services provided by a jurisdiction to its residents or other jurisdictions. Examples of downstream dependencies include the ability to provide critical functions such as issuing death and birth certificates, deeds for property sales, 911 services, elections, drinking and wastewater treatment, traffic control, information services, scheduling portals, registration services, and customer billing.

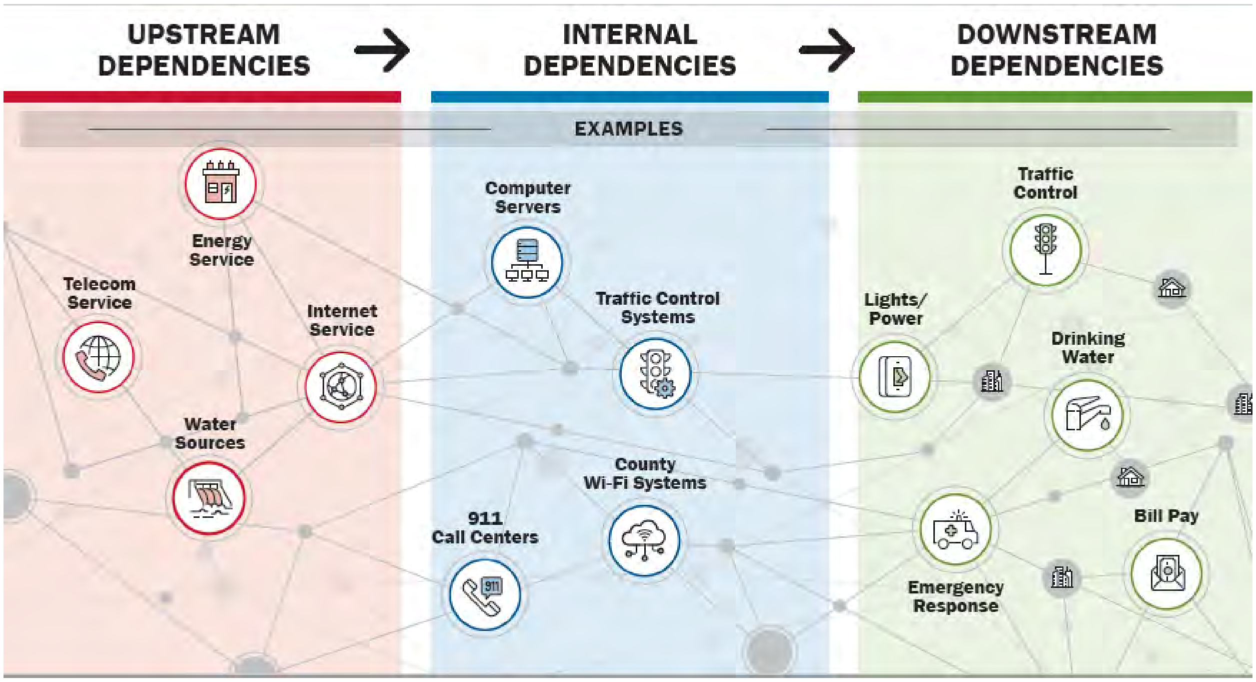


Figure 2: Examples of Upstream, Internal, and Downstream Dependencies

Questions to Assist in Identifying Dependencies

1. What are the service's external dependencies?

An external dependency exists when an outside entity (e.g., contractor, customer, service provider) has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to the critical service or its associated assets.

Examples of services provided to an organization from external entities may include: outsourced activities that support operation or maintenance of the critical service; security operations; IT service delivery and operations management or services that directly affect resilience processes; backup and recovery of data, provision of backup facilities for operations and processing and provision of support technology or similar resilience-specific services infrastructure providers such as power and dark fiber; telecommunications (e.g., telephony and data); technology and information assets (e.g., application software, databases); and education and training resources.

2. Which external dependencies are most important?

The intent of prioritization is to ensure that the jurisdiction properly directs its resources to the external dependencies that most directly impact the critical service.

Prioritization criteria may include dependencies that: directly affect the operation and delivery of the critical service; support, maintain, or have custodial care of critical service assets; support the continuity of operations of the critical service; save access to highly sensitive or classified information; support more than one critical service; supply assets that support the operation of a critical service; or impact the recovery time objective of the critical service.

3. On which infrastructure providers does the critical service depend?

Critical services may be dependent on infrastructure providers to remain viable. The organization may need to address the loss of these providers, which may affect the resilience of the critical service. The jurisdiction may need to consider the resilience of the providers when developing service continuity plans.

These infrastructure services may include telecommunications and telephone services, data and network service providers, electricity, natural gas and other energy sources, and water and sewer services.

Considering Cyber Dependencies

When identifying dependencies for critical services, it is important to consider the interconnected nature of the service and its components. Cyber dependencies exist both internally and externally to an organization and may be through direct or indirect relationships. For example, websites depend upon servers, data, and access to the internet. Jurisdictions might provide and maintain their own software, computers, and networks to operate their websites, which form an internal dependency, or contract with external website providers to manage their websites, forming an external dependency. External dependencies often exist when jurisdictions contract with external organizations to provide services such as computer support and security. A direct dependency exists between a utility control computer and a computerized sensor, while a logical but indirect dependency exists between natural gas delivery systems and their customer billing systems.

Questions to Consider when Identifying the Owner of a Cyber System

- What part(s) of the jurisdiction is responsible for the delivery of the critical service?
- Who are the owners of the assets required for delivery of the critical service?
- Are both owners and operators of assets documented?

3.2.3. IDENTIFYING THE CONSEQUENCES OF SERVICE LOSSES OR DISRUPTIONS

With an understanding of key dependencies, the planning team may identify the likely consequences of service interruptions caused by the loss or disruption of another service or cyber asset. As part of this process, it is important to determine whether the consequence would occur immediately after an incident or later. For example, a service might fail immediately if its industrial control computer failed because of an attack or system fault. Or, a service might fail after the depletion of a resource, such as a backup battery providing power during a power outage. Awareness of these consequences, and associated impacts to community lifelines, helps to establish incident response priorities and identify resources and capabilities that improve incident response and reduce the consequences of cyber incidents.

During this process, the planning team works with service owners and operators to understand the criticality of their dependencies on other services and cyber assets. This helps to identify the impact of the loss or disruption of these support services and cyber assets. In a cyber incident, cascading impacts are likely.

Sample Questions to Consider – Consequences of Service Loss or Disruption

- What happens if there is a sudden loss of access to servers with a municipality's email and contact data?
- What happens to the community water supply if the pumps lose electricity?
- What happens to the availability or quality of water if the industrial control systems or their communication networks are disrupted?
- What happens if the water treatment process is compromised by a malicious incident and the monitoring system is unable to show trustworthy, accurate testing results to human workers?
- What public health impacts may occur from the cyber incident? Are local healthcare facilities able to respond on a community-wide scale?
- What is the consequence if web-based services, such as scheduling and bill-payment, are unavailable because of a cyber incident that affects the computers or the network?
- Do impacted systems belong to a private company or a public entity?
- Are privately owned systems part of the critical infrastructure for the jurisdiction?
- What happens if financial information, such as customer credit card information, is stolen by a malicious actor?

As part of this process, the planning team may also determine how to gain situational awareness of the status and operational readiness of critical services during an incident so that information may be factored into plan development. Gaining this situational awareness will often depend on the managers of those services and cyber assets. While some services, such as water and electricity supply, are directly observable and customers will likely report losses, other services and cyber assets require the use of instruments that monitor and report on status. Additionally, service assessments might require personnel to check and report on operational readiness and whether services are affected by the cyber incident. The planning team engages with the owners and operators of critical services and assets to understand how status is monitored and communicated. This information is essential to the incident response, as it enables the emergency management team to understand what and how services are affected, what services are not affected, and what services might be affected later.

Planning ahead to quickly obtain information in a response may include:

- Establishing a partnership with a neutral, third-party intelligence organization (e.g., state/local fusion center, Multi-State Information Sharing and Analysis Center [MS-ISAC]);
- Establishing legal agreements among critical service providers to promote information-sharing; and;
- Creating anonymous reporting tools that scrub sensitive information while promoting shared visibility of the event or its impacts.

3.3. Prioritizing and Planning

Using information gained in the assessment process and documented in the critical services and dependencies inventory, the planning team appraises each cyber asset to determine how vital it is for the operation of critical services. The planning team, in close collaboration with the system owners and operators, discusses what redundancies or backups are available for those services if internet or web service connectivity is lost for a significant period of time. For example, some IT services may be able to be run manually or be relocated to a non-impacted location. Once these contingencies have been established, the planning team has a clearer understanding of what systems are essential, what is required to operate those systems, and what alternative methods are available for operating those services. The planning team uses this information to establish priorities for services, how to apply limited resources, and the order of response efforts prior to an incident.

The ordering of response efforts considers time-dependent aspects such as how long a service may remain unavailable or disrupted before causing a negative impact. During a response, the priorities may change rapidly as services become available or unavailable. These changes may indicate destabilization of community lifelines and be tracked and included in incident reporting products that support the reevaluation and determination of incident response priorities.

Cyber Risk Assessments Resources

- CISA Cyber Resilience Review Asset Management: Provides guidance on how to identify, document and manage assets to evaluate and improve cyber resilience and response.
- CPG 201: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide: Provides guidance on conducting THIRA and SPR assessments and evaluating levels of preparedness.
- FEMA National Risk and Capability Assessment: Provides guidance for assessing the risk of all threats and hazards.
- NIST Guide for Conducting Risk Assessments: Provides guidance for assessing cybersecurity risks of federal information systems and organizations.

4. Emergency Management Roles and Responsibilities

Emergency managers' roles and responsibilities in preparing for and responding to a cyber incident may differ from those associated with other incident types. Roles and responsibilities may also differ across jurisdictions based on existing authorities and plans. Some jurisdictions place the emergency management organization in the lead coordinating role for cyber incidents, while others identify IT or law enforcement entities as the primary coordinator. In those instances where emergency management is not the lead, emergency managers take on supporting roles focused on the consequence management related to impacts from the incident.

In many jurisdictions, the emergency manager is responsible for coordinating the development of a plan or annex focused on cyber incident response, and for factoring cyber considerations into other plans. This often includes the oversight and leadership of the planning team and ensuring the necessary representatives are engaged in the effort. See Appendix A for guidance on forming the core and collaborative planning teams, including cyber-specific considerations.

Emergency managers should understand the stages of a cyber incident (described in the Introduction to Cyber Incident Response Planning section of this guide and NIST's Computer Security Incident Handling Guide), as well as the relevant legal requirements or restrictions and the roles and responsibilities that are listed in the jurisdiction's cyber plan or annex, if available. Beginning with detection of a cyber incident, emergency managers have important responsibilities in the management of direct and indirect impacts. Similar to other technical hazards, emergency managers may not be expected to directly work on containing and eradicating cyber threats. To the greatest extent possible, response actions taken should avoid causing further damage or impacts to threat investigation and removal operations by cyber professionals. Emergency managers may also assist with communication procedures including notifying the appropriate people. They may also be able to help manage questions throughout an incident to ensure that timely remediation occurs for the affected organization. As the focus of the incident transitions to recovery[9], emergency managers coordinate with the cyber response team to verify that the threat is contained and with stakeholders to ensure that affected operations are restored.

During an incident, emergency managers prioritize resources, such as personnel, to address the needs of response. Depending on impacts of an incident, emergency managers may activate other plans (e.g., power outage, distribution management). Activation of other plans may require incorporation of additional partners into incident support and consequence management. While not required of SLTT agencies managing cyber incidents within their own jurisdiction and capabilities, supporting federal lines of effort helps to ensure a robust response[10]. Balancing these potentially

[9] For more information visit the NIST Guide for Cybersecurity Event Recovery at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[10] For more information on cyber incident identification and reporting, visit Appendix B: Cyber Incident Identification and Closing Processes.

competing operational demands and the potential for cascading effects on stakeholders may require the establishment of a unified coordination structure.

Unified Coordination Group (UCG)

A Unified Coordination Group (UCG) is the primary organizational structure for managing and supporting complex disaster response operations. Depending on the needs of the incident, a UCG is comprised of senior leaders representing jurisdictional interests and may include federal, state, local, tribal, or territorial governments; the private sector; or nongovernmental organizations. In coordination with applicable government and private entities, Emergency Support Function personnel assess the situation and identify requirements. Federal agencies may provide resources under mission assignments or their own authorities. The UCG applies unified command principles for coordinating the assistance provided to support the jurisdiction's response.

For instance, in 2016, Presidential Policy Directive on United States Cyber Incident Coordination (PPD-41, July 2016)[11] established lead federal agencies and an architecture for coordinating the broader federal government response to cyber incidents. PPD-41 created the Cyber UCG to serve as the primary coordinating structure among federal agencies in response to significant cyber incidents, as well as the integration of private sector partners into incident response efforts, as appropriate. The lead federal agencies for this UCG are the Department of Justice (acting through the Federal Bureau of Investigation), the Department of Homeland Security (acting through CISA) and the Office of the Director of National Intelligence. When cyber incidents threaten or result in physical consequences leading to a Stafford Act declaration, FEMA may serve in a combined Cyber/Physical UCG. Guided by the specific needs of an event, the Cyber UCG may involve additional federal agencies, SLTT governments, non-governmental organizations, international counterparts, and the private sector.

Considering the complex nature of cyber incidents and the high potential for cascading impacts, jurisdictions of all sizes may consider using a UCG structure to better organize response and recovery efforts to ensure that the priorities of various officials, subject matter experts, and asset owners are consistent and best meet the needs of the incident.

Emergency managers rehearse their roles and responsibilities for cyber incident response through customized scenarios and exercises. Such activities help the planning team explore contingencies, identify gaps, validate existing plans, and determine appropriate courses of action. Activities are iterative and build on prior incidents and exercises to strengthen jurisdictional capabilities. The incident examples below may be used to identify potential lead and supporting roles for emergency managers.

[11] Presidential Policy Directive on United States Cyber Incident Coordination, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Example Scenario #1: Compromised Water Systems

Early on the morning of November 5, 2020, a water treatment facility within Central City received a call from a customer complaining about their water: "I went to get some water from my kitchen sink, and it immediately smelled like bleach was coming out of the faucet. It tasted wrong, even after I tried boiling it for my morning coffee. Is it safe to drink the water?"

An inspector performs a manual measurement of the chlorine levels in the water system and verifies that the water contains too much chlorine. The investigation includes an examination of the control system that operates and monitors the water treatment process. The control system displays the settings that regulate the release of chlorine and monitor the levels of chlorine appear normal. All physical controls (e.g., gates, locks) are operating as expected.

The facility's IT department suspects a cyber actor tampered with the technical controls to release an abundance of chlorine but need time to verify their theory and to hire additional forensic professionals. They aren't ready to release information to staff or the press until they can confirm the source. The water treatment department issues a "Do Not Drink" Water Advisory to inform their customers that the water is contaminated with potentially harmful amounts of chlorine and boiling the water does not make it safe to drink.

Example Emergency Manager Lead Roles:

- □ Coordinating communication to identify the scope of the incident (e.g., what jurisdictions are impacted)
- □ Activating the emergency operations center
- □ Developing Incident Action Plans
- □ Coordinating with cyber authorities to maintain situational awareness and reporting
- □ Managing coordination of resource and support requests from responding agencies
- □ Organizing hazardous materials support to identify and secure contaminated areas
- □ Identifying the potential for cascading impacts or additional hazards following the incident
- □ Tracking capability gaps and strengths for improvement planning following the incident

Example Emergency Manager Supporting Roles:

- □ Communicating information about the incident to law enforcement and nearby jurisdictions
- □ Developing and distributing notifications to the public regarding impacts and status
- □ Coordinating safety and security of the impacted property, as necessary
- □ Engaging private sector partners to provide resources and technical support
- □ Coordinating the distribution of emergency supplies of potable water

Example Scenario #2: Tornado

Late in the evening of June 20, 2022, Central City experienced an intense thunderstorm that quickly intensified. Meteorologists issued a "Tornado Watch," and shortly after a "Tornado Warning" circulated throughout Central City. Within minutes, an EF-4 tornado touched down and caused widespread, severe damage to property and infrastructure. The tornado caused widespread electricity outages and the heavy rainfall caused widespread flooding.

Preliminary damage assessments indicate that several buildings that provide critical services for Central City were damaged by the tornado and their contents appear to have been exposed to the rain. These buildings house computer and communications systems that serve the jurisdiction. These cyber systems — computers, networks, and communications gear — may have suffered physical damage from the tornado, water damage from the rain, or electronic damage from lightning. Response teams are struggling to establish communications and coordination due to power outages and disruptions to communications systems in the area.

Example Emergency Manager Lead Roles:

- ☐ Activating pertinent emergency operations plans and/or annexes
- ☐ Advising senior officials regarding the situation and emergency/disaster declarations
- ☐ Identifying incident objectives and priorities in coordination with jurisdictional leadership
- ☐ Activating the emergency operations center
- ☐ Developing Incident Action Plans
- ☐ Assessing the storm's impact on the jurisdiction's critical services
- ☐ Communicating with the public about the status of key critical services and safety risks
- ☐ Coordinating response to and recovery from the loss of critical services
- ☐ Coordinating temporary emergency power at critical facilities and alternate communication resources needed for key services, such as 911 call centers
- ☐ Identifying the potential for cascading impacts or additional hazards following the storm
- ☐ Serving as a coordination point for response partners, supporting communication, incident command, and the development of a common operating picture
- ☐ Tracking capability gaps and strengths for improvement planning following the incident

Example Emergency Manager Supporting Roles:

- ☐ Providing situational awareness reporting
- ☐ Coordinating safety and security for impacted property, as necessary
- ☐ Coordinating with third-party vendors or suppliers with impacted property

Example Scenario #3: Insider Threat

While employed with Central City's publicly owned Power & Electric (P&E) Company, a billing specialist had administrator access to the computer systems used by city residents to pay gas and electric bills online. In early July 2021, the billing specialist was terminated from P&E, losing access to the company's computer systems. The billing specialist was irate over the termination, arguing that it was unfair and unjust. After receiving a final paycheck, in retaliation for the termination, the former employee used a fake user account that had previously been created while employed with P&E to log into the company's computer systems.

Once logged in through the fake user account, the former employee created a second fake user account and used it to edit approximately 50,000 records and delete approximately 1,000 records. Of particular concern, the former employee changed the accounts of numerous residents to appear that they were months delinquent in paying their utility bills, resulting in thousands of residents and businesses having their electricity incorrectly turned off. The edits and deletions are also disrupting the ability of city residents to pay their bills online. After taking these actions, the former employee deactivated both fake user accounts and logged out of the system.

Example Emergency Manager Lead Roles:

- ☐ Coordinating with P&E to maintain situational awareness and reporting
- ☐ Identifying the potential for cascading impacts or interruptions to the community's essential services
- ☐ Activating the emergency operations center
- ☐ Developing Incident Action Plans
- ☐ Tracking capability gaps and strengths for improvement planning following the incident

Example Emergency Manager Supporting Roles:

- ☐ Communicating information about the incident to law enforcement and nearby jurisdictions
- ☐ Developing and distributing notifications to the public regarding impacts and status
- ☐ Determining what activities are needed to support residents who have lost power, including those who are dependent on electricity for life sustaining medical needs
- ☐ Coordinating with mass care organizations to provide assistance to residents in the event that power restoration is delayed
- ☐ Engaging private sector partners to provide resources and technical support
- ☐ Coordinating the distribution of emergency resources, such as generators, as necessary

5. Communication Considerations

Communications during cyber incident response need to be carefully planned, and similarly to communication considerations for other incidents, include both information sharing among emergency management and incident response personnel, as well as messaging out to broader stakeholder groups and the general public. This section presents key considerations for communicating before, during, and after a cyber incident.

5.1. Integrated Communications

It is important to identify who will serve as the lead for communications in a cyber incident and how the communications will occur. As described in the National Incident Management System (NIMS), integrated communications are a foundational characteristic of incident command and coordination. "Integrated communications provide and maintain contact among and between incident resources, enable connectivity between various levels of government, achieve situational awareness and facilitate information sharing. Planning, both in advance of and during an incident, addresses equipment, systems, and protocols necessary to achieve integrated voice and data communications."[12] Impacts from cyber incidents may adversely affect voice and data communication channels, either by taking them down entirely or comprising the security of the system, necessitating alternative communication channels. Planning efforts consider and address reporting mechanisms for cyber incidents, the possibility of degraded communications, notification procedures for key stakeholders, and handling procedures for sensitive information.

- **Reporting:** The planning team identifies who is contacted in the event of a cyber disruption, what details are reported, and how that information is reported. Consideration is given to when the cyber incident should be reported to CISA. CISA encourages voluntary reporting. Consideration should also be given to when law enforcement is notified, such as if criminal activity is suspected or an act of cyber terrorism (cyber events that impact critical infrastructures), federal reporting processes, and any legal requirements related to notification.[13] For cyber incidents that may be malicious, it is best to ensure the reporting channel is outside the affected systems. For example, an organization that believes their systems are compromised would not use email. Instead, they might utilize a phone unaffiliated with the organization to ensure that their communications are not intercepted by the malicious actor.

- **Alternative Communications Systems**: Cyber incidents, regardless of cause, may render common voice and data communications channels unusable. It is important for the planning team to understand how their communication channels rely on cyber systems and how they may be impacted. The planning team identifies alternative communication mechanisms to use when needed and ensures all appropriate parties have the knowledge and access to effectively use

[12] National Incident Management System, Third Edition, October 2017.

[13] For more information on cyber incident identification and reporting, visit Appendix B: Cyber Incident Identification and Closing Processes.

those channels. For cyber incidents that may be malicious, responders identify communication channels that are separate from the impacted platform since threat actors may intercept sensitive information on compromised channels. CISA recommends developing and implementing a Primary, Alternate, Contingency, and Emergency (PACE) plan, which establishes options for redundant communications capabilities if an incident disrupts or degrades primary capabilities.[14]

- **Notification of Key Entities:** The planning team establishes procedures for identifying which stakeholders to notify in the event of a cyber incident (or how to determine which stakeholders to notify) and what information to communicate. It is best to pre-identify points of contact for communications, both internally and with key external partners. Aligning communications to the content required per CISA's incident reporting form and other key information may include:
    - Date of the incident;
    - Description of the incident;
    - Processes or services affected by the incident;
    - Actions taken so far to deal with the incident;
    - Any actions that the stakeholder may need to take; and
    - Contact information to receive further information.

- **Information Sharing**: As discussed in Engaging Service Owners and Operators section of this guide, communications before and during a cyber incident may require the sharing of sensitive information, necessitating the establishment of a confidentiality agreement, NDA, or other legal agreement such as a private-public partnership. Ideally, such an agreement is established before an incident occurs, though in some instances they may need to be developed during incident response. The planning team considers such requirements when developing their plan or annex and includes a procedure for quickly establishing such agreements when an incident occurs.

[14] For more information on Primary, Alternate, Contingency, and Emergency (PACE) planning, visit: https://www.cisa.gov/sites/default/files/2023-05/23_0426_ncswic_PACE-Plan_508.pdf.

National Emergency Communications Plan

The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen and enhance emergency communications capabilities. Its vision is to enable the Nation's emergency response community to communicate and share information securely across communications technologies in real-time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event.

The NECP establishes six strategic goals to drive progress toward the vision: Governance and Leadership; Planning and Procedures; Training, Exercises, and Evaluation; Communications Coordination; Technology and Infrastructure; and Cybersecurity. By adopting these goals, public safety organizations support three national priorities for advancing emergency communications: enhancing effective governance among partners with a stake in emergency communications, addressing interoperability challenges posed by rapid technology advancements and information sharing, and building a resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities. To learn more about the NECP, visit: https://www.cisa.gov/necp.

Priority Telecommunications Services

CISA provides a suite of communications services that enable public health and safety, national security, and emergency preparedness personnel to communicate with priority when networks are degraded or congested.

Government Emergency Telecommunications Service (GETS) provides emergency access and priority processing over wireline commercial telephone networks at no cost.

Wireless Priority Service (WPS) provides emergency access and priority processing over wireline commercial telephone networks at no cost.

Telecommunications Service Priority (TSP) Program is a Federal Communications Commission program, managed by CISA, which mandates that service providers prioritize the installation (provisioning) and restoration of critical voice and data circuits to facilities that support public health and safety, national security, and emergency preparedness.

Utilizing these services can improve continuity of communications and facilitate mission accomplishment. To register and learn more about Priority Telecommunications Services, visit: https://www.cisa.gov/about-pts.

5.2. Public Messaging

Some cyber incidents require notification of the general public. Given the sensitive nature of cyber incidents, it is important to establish clear procedures for public messaging before an incident occurs. Communication with the public requires awareness of what constitutes sensitive information and includes measures to ensure that sensitive information is protected. If available, a jurisdiction's Public Information Officers may provide assistance with developing and delivering important messages to their communities.

Sensitive Information[15]

Sensitive information can be defined as information that is restricted in some manner based on formal or administrative determination. Examples of such information includes contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and Personally Identifiable Information (PII).

Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Access restrictions may include NDAs. Information flow techniques and security attributes may be used to provide automated assistance to users that make sharing and collaboration decisions.

Not all cyber incidents are publicly reportable. Some may be deemed too sensitive for broader awareness. As such, public messaging protocols for cyber incidents should include steps to determine whether the incident may be publicly reported. For incidents that are reported publicly, ensure that notification regarding resolution of the incident is also distributed.

For those incidents that may be publicly reported, procedures should ensure that only necessary and appropriate information is included in messaging. Measures to ensure appropriate messaging to the public include:

[15] NIST, 2020, *Security and Privacy Controls for Information Systems and Organizations*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Table 1. Appropriate Public Messaging Considerations

DO	DON'T
▪ Determine whether law enforcement entities are more appropriate to develop and deliver messaging; ▪ Use clear and concise language; ▪ Identify any direct or indirect impacts to the safety and security of individuals; ▪ Focus on impacts to service availability; ▪ Emphasize actions that may be taken by the individual to lessen direct impacts; ▪ Emphasize actions that may be taken by the individual immediately to lessen cascading impacts from the initial incident; ▪ Encourage preparedness behaviors that build resilience for future incidents; and ▪ Distribute communications to those within the scope of service disruption	▪ Attribute the incident to any actors until definitive determination by a qualified incident response provider and coordination with federal government partners; ▪ Share specifics related to the location of facilities and assets that are impacted; ▪ Share specifics related to the nature and extent of damage to infrastructure assets; ▪ Identify any ongoing vulnerabilities that may be exploited by opportunistic attackers; ▪ Reference any specific data that have been breached before proper notifications have been made; and ▪ Share any Personally Identifiable Information (PII) or proprietary information

Sample Questions to Consider – Communications Service Loss or Disruption

It is crucial that jurisdictions' continuity assessments and plans include cyber considerations and utilize priority communications during times of degraded communications.

- Are all incident responders and decision makers enrolled in Priority Services, including GETS and WPS? Do they make regular test or training calls and incorporate Priority Services into their training and exercise programs?
- How will requests for TSP restoration be coordinated for any damaged communications services?
- Is the critical infrastructure subscribed to TSP?

Designed to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, the **Communications and Cyber Resiliency Toolkit** is an interactive graphic provided by CISA designed to assist in identifying ways to improve resiliency and develop plans for mitigating the effects of potential resiliency threats. To learn more, visit: https://www.cisa.gov/communications-resiliency.

6. Conclusion

Emergency managers play a central role in preparing jurisdictions for cyber incidents. By coordinating the efforts of planning team members, engaging with stakeholders, and ensuring effective communication, emergency managers develop an understanding of the cyber risks experienced by their jurisdictions and their potential impacts. This understanding and coordination allows for the development and ongoing validation of cyber incident plans, which increases the community's preparedness and overall resilience. Key aspects of cyber incident preparedness include:

- Understanding the types of cyber incidents likely to occur;
- Engaging service owners and operators;
- Identifying critical services and related dependencies;
- Prioritizing and planning for service and system disruptions;
- Clearly identifying roles and responsibilities; and
- Providing integrated communication and public messaging.

This guide aids SLTT emergency management personnel to collaboratively prepare for a cyber incident and support the development of a cyber incident response plan or annex. Appendix A provides details for developing a jurisdiction's cyber plan or supporting annex for an existing emergency operations plan. Appendix C shares additional resources on cyber policy, training, exercise, and funding options. Leveraged together, the information and resources in this guide empower emergency managers to address a persistent and complex hazard to ensure safe and resilient communities.

Appendix A: Developing a Plan

When preparing for cyber incidents, careful planning and collaboration are necessary to ensure a holistic and effective response. Using the six-step planning process detailed in CPG 101: Developing and Maintaining Emergency Operations Plans and shown in Figure 4, the planning team may develop a comprehensive and realistic plan or annex with purposeful involvement from all key stakeholders.

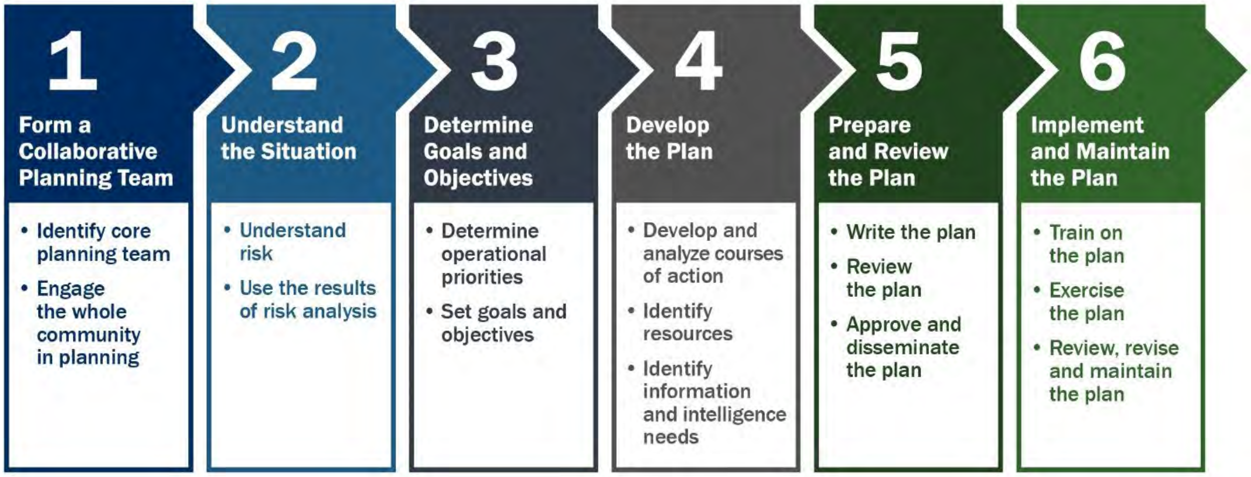

1
Form a Collaborative Planning Team
• Identify core planning team
• Engage the whole community in planning
2
Understand the Situation
• Understand risk
• Use the results of risk analysis
3
Determine Goals and Objectives
• Determine operational priorities
• Set goals and objectives
4
Develop the Plan
• Develop and analyze courses of action
• Identify resources
• Identify information and intelligence needs
5
Prepare and Review the Plan
• Write the plan
• Review the plan
• Approve and disseminate the plan
6
Implement and Maintain the Plan
• Train on the plan
• Exercise the plan
• Review, revise and maintain the plan

Figure 3. CPG 101 Emergency Operations Six-Step Planning Process

Step 1: Form a Collaborative Planning Team

The most realistic and complete plans result from a diverse planning team that includes representatives from across the whole community. Prior to identifying members of the broader collaborative planning team, it is necessary to identify the core planning team that will be responsible for leading coordination efforts. As CPG 101 suggests, the core planning team is composed of any key partners that are, “likely to be involved in most, if not all, responses.” Given the highly technical nature of cyber incident response, it is also important to include key cyber stakeholders on the core planning team.

The wide-reaching threat and impact of a cyber incident necessitate collaboration among many stakeholders in the planning process, to include emergency management, cyber professionals, legal advisors, law enforcement, private industry, and others. However, due to the technical challenges and elements posed by any cyber incident, an essential person to include on the core planning team is the senior information security officer. This could be the senior IT director, chief information officer (CIO), chief information security officer (CISO), chief technology officer (CTO), or designee. If an organization does not have someone with one of these titles, they may seek engagement from the applicable information security officer at the next highest jurisdictional level (e.g., local level, state level).

Once the appropriate information security officer is identified, the emergency manager may work with this individual to identify other members of the core planning team. It is beneficial to include members of the community that have a current understanding of the jurisdiction's continuity plans, cyber infrastructure and cyber security capabilities, as well as any critical connections, roles or features that otherwise would have been unknown. Table 1 below provides a list of individuals/organizations that may be beneficial to include on the core planning team.

Table 2 Potential Stakeholders for the Core Planning Team - Cyber

Individuals/Organizations	Expertise brought to Core Planning Team - Cyber
Emergency Manager or designee	▪ Experience coordinating multiple organizations with varying capabilities and areas of specialized knowledge ▪ Knowledge about all-hazards planning techniques ▪ Knowledge about existing mitigation, emergency, continuity, and recovery plans ▪ Knowledge of emergency communication and response systems that may require cyber systems ▪ Incident management experience and capabilities
Senior IT Director, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Technology Officer (CTO), or designee[16]	▪ Knowledge of cyber incident response ▪ Specialized personnel and support ▪ Knowledge of key cyber systems within jurisdiction (e.g., water treatment, traffic systems, energy connections, hospital systems, backups)
Senior Official (elected or appointed) or designee	▪ Government intent and priorities by identifying planning goals and essential tasks ▪ Authority to commit the jurisdiction's resources ▪ Knowledge of government resources
Police Chief or designee	▪ Knowledge about local laws and ordinances and specialized response requirements ▪ Knowledge about fusion centers and intelligence and security strategies for the jurisdiction ▪ Knowledge of key law enforcement requiring cyber systems (e.g., dispatch, records, emergency notifications)
Emergency Medical Services Director or designee	▪ Knowledge about emergency medical treatment requirements for a variety of situations ▪ Knowledge of key medical resources that require cyber systems (e.g., dispatch, dispensing)

[16] This is an essential member of the core planning team. If the organization does not have someone with one of these titles, the emergency manager or senior official would seek engagement from the applicable information security officer at the next highest jurisdictional level (e.g., county level, state level).

Individuals/Organizations	Expertise brought to Core Planning Team - Cyber
Fire Chief or designee	▪ Knowledge about the jurisdiction’s fire-related risks ▪ Knowledge of key fire resources that require cyber systems (e.g., dispatch)
Public Works Director or designee	▪ Knowledge about the jurisdiction’s road and utility infrastructure and the cyber-based systems in use (e.g., traffic systems, road signage)
Public Health Officer or designee	▪ Understanding of the unique medical needs of the community
General counsel or legal advisor	▪ Knowledge of applicable data privacy laws and other legal requirements

Given the potential reach and scope of a disruptive cyber incident, it is important to include additional community stakeholders in the planning process through the broader collaborative planning team, including those associated with community lifelines and other critical services that rely on cyber systems. Examples of key stakeholders that may be beneficial to include on the broader collaborative planning team are presented in Table 2.

Table 3. Potential Stakeholders for the Collaborative Planning Team - Cyber

Individuals/Organizations	Expertise brought to Collaborative Planning Team - Cyber
Utility representatives or designee	▪ Knowledge about utility infrastructure and possible cyber interdependencies (e.g., connections to and from gas, electric, and water interconnections)
Hazardous Materials Coordinator or designee	▪ Knowledge about hazardous materials that are produced, stored, or transported in or through the community, and the cyber-based systems in use (e.g., facility controls, machinery)
Transportation Director or designee	▪ Knowledge about the jurisdiction’s road infrastructure and transportation resources and the cyber-based systems in use (e.g., traffic systems, camera operations)
School Superintendent or designee	▪ Knowledge about the hazards that directly affect schools and the cyber-based systems in use (e.g., administrative systems, communication software, enrollment information)

Individuals/Organizations	Expertise brought to Collaborative Planning Team - Cyber
Local federal response partners or designee, to include Protective Security Advisors/Cyber Security Advisors and others[17]	▪ Knowledge about specialized personnel and equipment resources that could be used in an emergency (e.g., CIRT teams) ▪ Knowledge about potential threats to or hazards at federal facilities ▪ Knowledge of regional interconnections and partnerships that may be able to assist with a cyber incident ▪ Understanding of broader level threat landscape that may be required for overall containment of cyber threat
Nongovernmental organizations and other private, not-for-profit, faith-based, and community organizations or designee	▪ Knowledge about community resources and needs ▪ Understanding of community and its communication needs (e.g., case management systems)
Local business and industry senior IT representatives or designee	▪ Knowledge of their IT infrastructure and their dependencies (e.g., cash system, security system, communications)

Step 2: Understand the Situation

In this step, the planning team develops an understanding of how potential incidents may occur in and impact their community. Information in the Types of Cyber Incidents section of this guide provides a starting point for understanding the common types of cyber incidents and how they could impact the community. The Assessing Cyber Risks to Inform Prioritization and Planning section provides guidance and considerations for identifying potential consequences and impacts from cyber incidents and restoration priorities.

The planning team may benefit from developing a few scenarios to drive their planning efforts. Not every cyber incident will require a broad community response, or even a response outside the affected entity. Developing and exploring different scenarios helps the planning team understand the potential risks to be addressed in the response plan or annex and to examine the dependencies of assets and services. Exercises may also be used after the plan is developed to identify potential gaps and highlight where additional training and coordination is needed.

Prior to developing a cyber incident plan or annex, or integrating cyber incidents into a jurisdiction's emergency operations plan (EOP), the planning team should fully understand their EOP and any

[17] PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts who facilitate local field activities in coordination with other Department of Homeland Security offices. They also advise and assist state, local and private sector officials and critical infrastructure facility owners and operators. For more information visit: https://www.cisa.gov/protective-security-advisors.

existing supporting plans and annexes, such as communications and energy. Annexes supplement and are consistent with the EOP and do not duplicate or conflict with it. A jurisdiction's EOP base plan or supporting plans will address many responsibilities and actions taken when implementing cyber incident response, as these actions are frequently required regardless of the specific threat or hazard. A cyber annex therefore addresses the unique characteristics and requirements not already covered in the EOP base plan or other annexes.

Step 3: Determine Goals and Objectives

In this step, the planning team works together to determine operational priorities and then sets goals and objectives for cyber incident response. Operational priorities specify what the responding organizations intends to accomplish and the desired end-state for the cyber incident response. Using the scenarios and risk analysis results from Step 2, the planning team engages the senior official (e.g., tribal leader[s], mayor, county judge, commissioner[s]) to explore how the incident and impacts may evolve within the jurisdiction and what defines a successful outcome. The resulting discussion explores the requirements necessary to achieve the desired end-state, which will help determine actions and resources needed for the incident response. Senior officials may identify the desired end-state and operational priorities for cyber incident response operations or affirm those proposed by the planning team.

The actual situation when an incident occurs will determine the incident objectives. The goals and objectives established in the EOP are based on planning assumptions and provide a starting place for incident response planning.

Once operational priorities for the EOP or annex are set, the planning team collectively determines goals and objectives for cyber incident response. The goals and objectives should be realistic and based on the current state of cyber maturity in the jurisdiction. When crafting goals and objectives, the planning team considers the minimum capabilities needed to provide essential services and understands that priorities may change during the course of the incident.

Possible Goals for a Cyber Incident Response Plan May Include:

- Ensure continuous operations of community lifelines and critical services.
- Disseminate timely information to the community regarding impacted services, restoration expectations, and available support.
- Efficiently exchange information with service owners/operators to enable rapid response and recovery efforts.
- Mitigate additional cascading impacts by isolating the impacted system(s), if possible.
- Identify how the system was compromised and make the immediate changes to ensure vulnerabilities cannot continue to be exploited while containment and recovery efforts are ongoing.

Step 4: Develop the Plan

Based on the results of Steps 2 and 3, the planning team may begin developing their plan, to include generating, comparing, and selecting possible courses of action to achieve the identified goals and objectives and identifying resources. Planners may refer to CPG 101 for writing and reviewing checklists, as well as format considerations.

The cyber experts on the planning team play an essential role in developing and evaluating courses of action, as they may provide insight into the likely actions, impacts, and decision points in a cyber incident. When developing courses of action, the planning team may follow the process described in CPG 101. During this decision process, the planning team considers:

- The roles and responsibilities each party may play throughout a cyber incident. For example, an emergency manager may provide support in an emergency caused by a cyber incident or may be responsible for leading the response if the cyber incident resulted in physical damages to water treatment or fuel supply facilities;
- A timeline of when expected response parties would be available;
- Specific types of cyber incidents that would require special notifications or cause concern that may require notification to legal authorities, neighboring jurisdictions, state, or federal governments; and
- When to ask for additional specialized assistance and determine what options are available.

When developing courses of action, the planning team considers any applicable legal requirements or procedures. Cyber incidents, such as those involving data breaches, may necessitate compliance with specific legal reporting requirements. Laws might specify when and how to disclose privacy or identify risks, such as the breach of private personal information. For example, if a data breach affects financial information such as payment (credit/debit) cards, the organization may need to notify consumer reporting agencies and the payment card issuers and processing companies.

Considering an Effects-Based Approach

When planning for a cyber incident, it can be difficult to predict the impact of cascading failures across infrastructures because unknown and unintended consequences are probable, given the ever-increasing complexity and connectedness of infrastructure. As such, jurisdictions may benefit from considering the potential effects of an incident when developing and selecting courses of action. These effects often fall into at least one of the following categories: loss of power, loss of internet, loss of local networks, loss of voice communications, loss of local IT equipment, loss of access to data, and loss of key IT personnel.

Effects-based planning can serve as a vehicle to bring together disparate groups to focus on how to strengthen response posture and improve resiliency.

After selecting courses of action, the planning team determines what resources are necessary to carry out the associated activities and identifies resource gaps so that they may work with partners to preemptively address those gaps. The planning team may use capability estimates to describe the jurisdiction's ability to perform a course of action. When developing capability estimates for cyber incident response planning, the planning team may want to consider:

- Cyber Incident Response Teams (CIRT);
- State/federal partners;
- Mutual aid assistance;
- Third-party cyber advisors, which may be private sector partners;
- Computer equipment (e.g., laptops, monitors, networking);
- Industrial control system hardware (e.g., human machine interfaces);
- Communications (e.g., telephone, network); and,
- Computer storage (e.g., hard drives).

Establishing a Cyber Disruption Team (CDT)

Jurisdictions may want to consider establishing a CDT in their plan. A CDT is a specialized consultative group comprised of representatives and subject matter experts from emergency management, IT, law enforcement, critical infrastructure, and other relevant domains. The CDT is a key resource for understanding:

- the nature and potential durations of cyber disruptions;
- the effects of cyber disruptions on critical life-safety, critical cyber assets, and other key response activities; and
- the potential resource needs of IT personnel and agencies to maintain, protect, and re-establish operations.

During cyber disruptions of any nature, the CDT will integrate into the Incident Command System (ICS) structure of the overall incident response. Utilizing the CDT framework incorporates the added benefit of integrating emergency management principles and procedures for IT personnel and other disciplines.

Depending on the impacts of an incident, emergency managers may need to activate other plans or annexes (e.g., power outage, distribution management). Activation of other plans may require incorporation of additional partners into incident support and consequence management functions. Establishing a unified coordination structure aims to effectively integrate partners with leadership roles into a complex cyber incident that includes extensive cascading impacts.

During this step, the planning team also determines how to assess the status and operational readiness of the previously identified essential services and cyber assets and factors that information into plan development. This will help when responding to cyber incidents by providing emergency managers with information about what and how services are affected, what services are not affected, and what services might be affected later.

Step 5: Prepare and Review the Plan

This step involves translating the findings of Steps 3 and 4 into a cyber incident response plan or annex, reviewing it to ensure that it meets applicable regulatory requirements and jurisdictional standards, verifying that it is useful in practice, and obtaining approval on the plan by the appropriate authorized body. During this step, jurisdictions may update key stakeholders and receive buy-in from partners. Planners may follow the best practices for plan development outlined in CPG 101 to ensure the plan is readily understood by all audiences regardless of their technical expertise.

To ensure the plan meets regulatory requirements and standards, the planning team may engage external partners (e.g., the next level of government, regional or national cyber experts) to perform a review of the document. To evaluate the effectiveness of the plan, the planning team may consider the five criteria outlined in CPG 101: adequacy, feasibility, acceptability, completeness, and compliance.

Questions to Consider When Reviewing a Cyber Incident Plan or Annex

- Did the planning team include representation from the jurisdiction’s technology teams?
- Does the plan outline the roles and responsibilities of the key stakeholders?
- Does the plan map interdependencies between critical cyber systems or services?
- Does the plan include an emergency contact list for each of the critical cyber services?
- Does the plan identify potential consequences of service disruptions?
- Does the plan outline minimal service levels needed to maintain continuity of operations?
- Does the plan clearly identify available cyber response resources (e.g., personnel, administration and finance, operational organizations, logistics, communications, equipment, facilities)?
- Does the plan specify how to notify emergency management of an event with potentially cascading impacts to other areas?
- Does the plan identify when to escalate emergency response and who is responsible for making that decision?
- Does the plan clearly define the beginning and end of cyber incident response operations?
- Does the plan clearly define who is the lead, who are the support roles, and how to divide and address necessary tasks during cyber incident response?
- Does the plan include provisions for engaging private sector organizations in the management of cyber incident response either as resources or as members of the unified coordination group?
- Does the plan account for updates in technology since the last revision?

Prior to distributing the approved cyber incident response plan or annex, the planning team would confirm that the document does not contain any sensitive information that could be leveraged to carry out a cyberattack. Sensitive information may need to be redacted, or the plan's distribution limited to a smaller, specific audience as described earlier in the Communications Considerations section.

Step 6: Implement and Maintain the Plan

This step focuses on ensuring key stakeholders are familiar with the roles and processes described in the plan or annex, through training and exercises, and that the plan or annex is regularly updated to reflect lessons learned and best practices.

Training on the cyber incident response plan or annex is crucial to preparing the response team for timely communication and coordination activities. Routine training also helps ensure new staff are aware of their roles and responsibilities. It may be beneficial for trainings to address:

- Foundational cyber topics (e.g., common causes of cyber incidents, key terms);
- Basic topics in emergency management (e.g., planning, situational awareness, Incident Command System) for other key personnel (e.g., IT staff, CISO);
- Use of specific, essential response tools (e.g., decision support matrices, escalation criteria);
- Complex or nuanced aspects of response (e.g., notification, escalation, legal reporting requirements); and,
- Plan specific training (e.g., communication relay, role/function assignments).

Like other emergency plans and annexes, cyber incident response plans are exercised regularly. Use of Homeland Security Exercise and Evaluation Program (HSEEP) guidance can maximize the effectiveness of exercise development. Once exercise scope, objectives, and capabilities are identified, exercise planners may develop scenarios for their exercise. It is important for the exercise planning team to include cyber experts in both the exercise planning and after-action processes. These cyber experts help to ensure the cyber aspects of the exercise are realistic while understanding and interpreting the more nuanced aspects of a cyber incident so improvement actions are documented accurately. Jurisdictions may select to integrate cyber considerations into their broader exercise program, to include the Integrated Preparedness Planning Workshop and resultant multi-year Integrated Preparedness Plan recommended in the Homeland Security Exercise and Evaluation Program.

Michigan Statewide Cyber Disruption Exercise

As part of an annual scenario-based exercise series on cyber disruptions, Michigan conducted a functional exercise in 2021 to test the state's ability to respond to a simultaneous cyber-attack on multiple local governments and K-12 schools. The scenario was based on threat models, indicators of compromise, and actual events in Michigan and other states.

The exercise goals provided a scenario that grew in complexity and allowed teams to exercise response, interagency coordination, and communication capabilities. The exercise itself involved players from planning team organizations, local governments, and school districts.

Exercise planning included multiple organizations providing complimentary and overlapping skillsets, but with different capabilities and reporting structures. Preparation for the exercise included coordination among the major players to ensure mutual understanding and documentation of capabilities, command structures, and activation procedures.

Major planning organizations and key functions related to the exercise included:

- Michigan State Police Emergency Management and Homeland Security Division (MSP/EMHSD), responsible for emergency operations coordination and the State Emergency Operations Center;
- MSP Michigan Cyber Command Center (MC3), responsible for cyber emergency response coordination during critical incidents in the state;
- Michigan Department of Technology, Management, and Budget (DTMB) resources, including the Michigan Cyber Civilian Corps, trained technical experts who volunteer to local incidents when requested; and Michigan Cyber Partners, a collaboration of various state and local public entities who help local entities prepare for cyber incidents;
- Michigan National Guard, provides advanced cyber defense capabilities available to support state government and civilian industry; and
- Federal agencies including CISA and the FBI who work closely with state and local partners and provide national context to local incidents.

Highlights and lessons learned from the exercise:

- The planning process for the exercise allowed for state cyber response plans to be updated simultaneously;
- Experiences were applied in 2022 when using the Michigan Cyber Disruption Response Plan to aid in real-world interagency coordination and communication regarding the Russian/Ukrainian war and cybersecurity related threats to the state.
- The cycle of planning, training, and exercising together was essential to gain knowledge, understand organizational capabilities, close capability gaps, and build trusted relationships.

Exercise Resources

- The Homeland Security Exercise and Evaluation Program (HSEEP): Provides a set of guiding principles for exercise and evaluation programs, including a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Utilizing HSEEP helps to ensure a coordinated and comprehensive approach to planning, training, and strengthening capabilities ahead of a cyber incident.
- National Exercise Program (NEP) is a two-year cycle of exercises across the nation that examines and validates capabilities in all preparedness mission areas. SLTT jurisdictions are eligible to submit requests for exercise support and participate in the NEP.
- HSEEP After-Action Report Template: Provides a flexible template for after action report development.
- CISA Tabletop Exercise Packages (CTEPs): A comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Packages include cybersecurity Situation Manuals (SITMANs) covering topics such as industrial control systems (ICS), ransomware, insider threats, phishing, and elections-related cyber threat vectors.

Appendix B: Cyber Incident Identification and Closing Processes

The planning team works together to establish a process for monitoring, identifying, and declaring a cyber incident. The planning team identifies benchmarks or triggers that clearly indicate when the cyber incident plan or annex is activated. As a starting point for this effort, it may be helpful for the planning team to review the Cyber Incident Severity Schema in the National Cyber Incident Response Plan (NCIRP), which serves as a way to describe the severity or impact of a cyber incident.

For cyber-driven events, the first partners to notified often vary based on the incident and jurisdiction. This means that building strong relationships and understandings of cascading impacts from cyber incidents may enhance the capacity to make joint and informed decisions. Establishing relationships and reviewing cyber incident response protocols with these types of partners helps emergency managers gain an understanding of the types of situations they would be asked to assist or lead for a cyber-driven event. To report a cyber incident to CISA visit the Incident Reporting System.[18]

The planning team may also choose to establish benchmarks or triggers that signal the end of cyber incident response operations and a return to regular activities. For instance, a cyber incident response may end once the root cause of the incident has been identified and remediated or the situation stabilized. Cyber incidents often escalate and de-escalate differently than natural hazards. For example, while hurricanes often come with significant pre-warning and progress in severity, cyber incidents may have unexpected and immediate severe impacts. Similarly, other disasters may include a long-term recovery process that lasts months or years. Although cyber professionals may consider a cyber incident fully recovered once the compromised system is restored to functionality, the physical and cascading impacts of a cyber incident may require a longer recovery process. Open and regular communication among staff is key to understanding how similar terms are used in different organizations and for establishing clear expectations.

The end of a cyber incident may be hard to define, as it may blend into traditional recovery activities. Officially closing a cyber incident indicates that the situation has stabilized and allows for regular activities.

[18] https://www.cisa.gov/forms/report.

Cybersecurity Incident & Vulnerability Response Playbooks

CISA developed two playbooks to strengthen cybersecurity response practices and operational procedures for the federal government, public, and private sector entities. Building on insights from previous incidents and incorporating industry best practices, the playbooks contain checklists for incident response, incident response preparation, and vulnerability response that any organization can adapt to track necessary activities to completion.

- The Incident Response Playbook applies to incidents that involve confirmed malicious cyber activity and for which a major incident has been declared or not yet been reasonably ruled out.
- The Vulnerability Response Playbook applies to any vulnerability used by adversaries to gain unauthorized entry into computing resources. This playbook builds on CISA's Binding Operational Directive 22-01 and standardizes the high-level process that is followed when responding to vulnerabilities that pose significant risk across the federal government, and private, and public sectors.

To view the playbooks visit: Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (cisa.gov).

Appendix C. Additional Resources

Cyber Incident Management Guidance, References, and Training

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

- Emergency Directives and Binding Operational Directives: Provide actionable guidance in response to specific cybersecurity threats. Although Binding Operational Directives (BODs) and Emergency Directives (EDs) strictly apply to and require action from Federal Civilian Executive Branch agencies, the threats they address often extend to every sector. Therefore, CISA recommends all stakeholders review and adopt BOD and ED guidance.

- Binding Operational Directive 22-01: Establishes a CISA-managed catalog of known exploited vulnerabilities that carry significant risk to the federal enterprise and establishes requirements for agencies to remediate any such vulnerabilities.

- CISA Vulnerability Scanning: Provides automated vulnerability scans and delivers a weekly report, which helps secure internet-facing systems from weak configurations and known vulnerabilities.

- Cyber Essential Element -- Your Crisis Response: Provides tips focused on limiting damage and quickening restoration of normal operations.

- Cyber Essentials Starter Kit: Provides guidance for leaders of small businesses and small and local government agencies to help them start implementing organizational cybersecurity practices.

- Cybersecurity Glossary: A glossary of common cybersecurity words and phrases.

- Cyber Resilience Review (CRR): A no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by the Department of Homeland Security (DHS) cybersecurity professionals. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

- Cyber Incident Resource Guide for Governors: Information for governors and their staff on how to request federal support during or following a cyber incident.

- Cyber Incident Response Resources: Provides an overview of CISA's role in cyber incident response and includes supporting resources.

- Cyber Incident Response Training: No-cost cybersecurity incident response training for government employees and contractors across federal and SLTT government, and educational and critical infrastructure partners.

- Cybersecurity Performance Goals: Provide baseline IT and OT security practices that can improve resilience against, and meaningfully reduce the likelihood and impact of, known cyber risks and common TTPs.

- Cyber Security Evaluation Tool (CSET): Provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET includes the Cybersecurity Performance Goals Assessment, which organizations can use to evaluate their cybersecurity posture and drive investments towards meaningfully reducing the likelihood and impact of known risks and adversary techniques.

- Emergency Services Sector Cybersecurity Framework Implementation Guidance: Provides foundational guidance for how emergency services sector organizations may enhance their cybersecurity using the NIST Cybersecurity Framework.

- Emergency Services Sector Cybersecurity Initiative: Provides resources to help those in the emergency services sector better understand and manage cyber risks.

- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: Two playbooks developed by CISA to strengthen cybersecurity practices and operational procedures for the federal government, and public and private sector entities. The playbooks contain checklists for incident response, incident response preparation, and vulnerability response.

- Free Cybersecurity Services and Tools: Identifies free cybersecurity tools and services to help organizations further advance their security capabilities.

- Resources for State, Local, Tribal and Territorial (SLTT) Governments: Presents key resources for SLTT governments pertaining to cybersecurity, including best practices, case studies, and an SLTT Toolkit.

- State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) Cyber Resource Compendium: Identifies some of the major references that may help build or strengthen an organization's cybersecurity program.

- Tabletop Exercise Packages (CTEPs): A comprehensive set of resources designed to assist stakeholders in conducting their own exercises. The packages include cybersecurity situation manuals covering topics such as industrial control systems, ransomware, insider threats, phishing, and elections-related cyber threats.

FEDERAL EMERGENCY MANAGEMENT AGENCY

- Building Private-Public Partnership Guide: Provides best practices for jurisdictions to establish and maintain a private-public partnership, which is essential to successful cyber incident response.

- Continuity Resources and Technical Assistance: Information and tools on continuity of operations plans, assessments, and resources.

- Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans: Details the six-step planning process for developing emergency operations plans and hazard specific annexes.

- Comprehensive Preparedness Guide (CPG) 201: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Guide (SPG): Provides guidance for communities on conducting THIRA and SPR assessments and evaluating levels of preparedness.

- Homeland Security Exercise and Evaluation Program (HSEEP): Provides a set of guiding principles for exercise and evaluation programs, including a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.

- HSEEP After-Action Report Template: Provides a flexible template for after action report development.

- National Exercise Program (NEP): A two-year cycle of exercises across the nation that examines and validates capabilities in all preparedness mission areas. SLTT jurisdictions are eligible to submit requests for exercise support and participate in the NEP.

- National Incident Management System: Guides all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents by providing the whole community with shared vocabulary, systems, and processes.

- Preparedness Grants Manual: Describes regulations, policies, and procedures for managing preparedness grants with guidance specific to each grant. Includes information on the Homeland Security Grant Program.

- Threat and Hazard Identification and Risk Assessment (THIRA): Provides guidance for assessing the risk of all threats and hazards.

NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

- Computer Security Incident Handling Guide: Assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.

- Cybersecurity Framework: Provides strategic guidance to help build and execute a cybersecurity program. Helps organizations assess cyber risks and set plans for improving or maintaining their security posture.
- Guide for Conducting Risk Assessments: Provides guidance for conducting risk assessments of federal information systems and organizations.
- Guide for Cybersecurity Event Recovery: Provides guidance to help organizations plan and prepare for recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.
- Security and Privacy Controls for Information Systems and Organizations: Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, and other organizations from a diverse set of threats and risks.

OTHER RESOURCES

- Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government: Explains when, what, and how to report a cyber incident to the federal government.
- Data Breach Response Guide: Provided by the Federal Trade Commission and provides general guidance for an organization on how to manage a data breach.
- National Cyber Incident Response Plan (NCIRP): Maintained by the Department of Homeland Security, the NCIRP is a national approach to dealing with cyber incidents. It addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response.

Direct Resources and Partnerships

MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER (MS-ISAC)

In addition to working to help improve the cybersecurity posture of SLTT governments, MS-ISAC operates a cybersecurity operations center 24 hours a day, 7 days a week to provide real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

The MS-ISAC Cyber Incident Response Team (CIRT) provides SLTT governments with malware analysis, computer and network forensics, code analysis/mitigation, and incident response. External vulnerability assessments are also available after an incident. This service helps victims of cyber incidents to check if their remediation efforts have been effective. For more information, visit: https://www.cisecurity.org/ms-isac/.

SLTT government representatives who believe they are experiencing a cybersecurity event may report it to: https://www.cisecurity.org/isac/report-an-incident.

CYBER SECURITY ADVISORS (CSA)

CSAs are regionally located DHS personnel who direct coordination, outreach and regional support to protect cyber components essential to the sustainability, preparedness and protection of the Nation's critical infrastructure and SLTT governments. CSAs offer immediate and sustained assistance to prepare and protect SLTT and private entities. CSAs bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer coordination with the federal government. CSAs represent a front-line approach and promote resilience of key cyber infrastructures throughout the U.S. and its territories. For more information about CSAs, please email cyberadvisor@hq.dhs.gov.

EMERGENCY COMMUNICATIONS COORDINATORS (ECC)

ECCs are subject matter experts located across the country who build trusted relationships, enhance collaboration, and stimulate the sharing of best practices and information between all levels of government, critical infrastructure owners and operators, and key non-government organizations. ECCs seek to build partnerships between federal, state, local, tribal, and territorial government stakeholders as well as the private sector. These partnerships result in a united effort to improve the Nation's operable and interoperable emergency communications. For more information on the Emergency Communications Coordination Program, please visit: https://www.cisa.gov/emergency-communications-coordination-program.

PROTECTIVE SECURITY ADVISOR (PSA)

PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts. Operating under CISA's Integrated Operations Division, PSAs facilitate local field activities in coordination with other DHS offices while assisting state, local, private sector, and critical infrastructure officials, owners and operators. The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing. For more information about PSAs, visit: https://www.cisa.gov/security-advisors.

PUBLIC INFRASTRUCTURE SECURITY CYBER EDUCATION SYSTEM (PISCES)

PISCES is a non-profit organization that, in partnership with DHS CISA and the Pacific Northwest National Laboratory, partners with the private sector, colleges and universities, and local governments to provide no-cost cybersecurity event monitoring to small public sector organizations. Students leverage data collected from customer networks to build their skills as cybersecurity analysts, and report confirmed or potential compromises to the customer jurisdiction when identified. For more PISCES information, visit: pisces-intl.org.

Funding Considerations

ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT

The Robert T. Stafford Disaster Relief and Emergency Assistance Act[19] (Stafford Act) authorizes the President to declare a major disaster or emergency and provide federal assistance to states, territories, local governments, tribal nations, individuals and households and nonprofit organizations to respond and recover from a major disaster. All requests for a declaration by the President are made by the governor or tribal leader of the affected state, territory, or tribal nation. These requests are based on findings that "the disaster is of such severity and magnitude that effective response is beyond the capabilities of the State and the affected local governments, and that Federal assistance is necessary."

Cyber incidents may or may not meet the criteria for declaring a major disaster or emergency. During a cyber incident response, jurisdictions may need additional resources including computer hardware, software, cybersecurity services from vendors, and other support services or personnel. Planning for a potential widespread cyber incident, including the identification of various resource and funding sources, is critical for jurisdictions.

HOMELAND SECURITY PREPAREDNESS GRANTS

The Homeland Security Grant Program includes a suite of risk-based grants to assist state, local, tribal, and territorial efforts in preventing, protecting against, mitigating, responding to, and recovering from acts of terrorism and other threats. These grants provide grantees with the resources required for implementation of the National Preparedness System and working toward the National Preparedness Goal (NPG) of a secure and resilient nation.

In addition to other items allowed under the grants, certain cybersecurity planning, risk reduction activities, and hardware and operating system software designated for use in an integrated system, may be allowable under specific grant programs. Such systems include detection, communication, cybersecurity, and geospatial information systems.

For more information on Homeland Security Grants, visit:
https://www.fema.gov/grants/preparedness/homeland-security#programs.

CYBERSECURITY GRANT PROGRAMS

The passage of the Infrastructure Investment and Jobs Act of 2021 established the State and Local Cybersecurity Grant Program (SLCGP) and Tribal Cybersecurity Grant Program (TCGP). Implemented by CISA and FEMA, CISA serves as a programmatic subject matter expert for the programs, while FEMA provides grant administration and oversight for appropriated funds. For the SLCGP, state and territorial governments are responsible for cybersecurity planning and project development as well

[19] Pub. L. No. 93-288, as amended, 42 U.S.C. 5121 et seq.

as pass-through responsibilities to include distributing awarded funds to local governments to address cybersecurity risks and threats to information systems owned or operated by or on behalf of state, local, tribal, and territorial governments. For the TCGP, the tribal governments are recipients responsible for cybersecurity planning and project development, but no required pass-through of funding to other entities.

The overarching goal of the programs is to assist state, local, tribal, and territorial governments in managing and reducing systemic cyber risks. To accomplish this, CISA established four separate, but interrelated objectives:

- **Governance and Planning:** Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure the continuity of operations.
- **Assessment and Evaluation:** Identify areas for improvement in SLTT cybersecurity posture based on continuous testing, evaluation, and structured assessments.
- **Mitigation:** Implement security protections commensurate with risk through best practices.
- **Workforce Development:** Ensure organizational personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.[20]

For more information on the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program, email FEMA-SLCGP@fema.dhs.gov or FEMA-TCGP@fema.dhs.gov or visit https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program or https://www.cisa.gov/cybergrants.

CYBER RESPONSE AND RECOVERY FUND

The passage of the Infrastructure Investment and Jobs Act also included the Cyber Response and Recovery Act (CRRA), which authorizes the Secretary of Homeland Security to declare a significant cyber incident under specific circumstances. The CRRA also establishes the Cyber Response and Recovery Fund (CRRF), which CISA can use following a declaration to coordinate asset response activities, provide response and recovery support for the specific significant incident (including through asset response activities and technical assistance), and, as the CISA Director determines appropriate, award grants or cooperative agreements to help entities respond to or recover from the specific significant incident. Once the grant program is established, it will be implemented by CISA. After the program is established and implemented, CISA will provide more information to the public on the circumstances under which a grant can be awarded.

[20] https://www.nist.gov/itl/applied-cybersecurity/nice

Appendix D: Glossary

- **Asset**: Items of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation).

- **Attack**: An attempt to gain unauthorized access to system services, resources or information, or an attempt to compromise system integrity.

- **Confidentiality**: A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

- **Continuity Plan:** A documented plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of incidents that impact normal operations.

- **Cyber Incident**: An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

- **Cyber Infrastructure**: Electronic information, communications systems, services, and the information contained therein.

- **Cybersecurity**: The activity or process, ability or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

- **Data Breach**: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

- **Denial-of-Service (DoS)**: An attack that prevents or impairs the authorized use of information system resources or services.

- **Disruption**: An event which causes unplanned interruption in operations or functions.

- **Distributed Denial-of-Service (DDoS)**: A denial of service technique that uses numerous systems to perform the attack simultaneously.

- **Downstream Dependencies:** Services provided by a jurisdiction to its residents or other jurisdictions.

- **Exploit**: A technique to breach the security of a network or information system in violation of security policy.

- **Incident Command System (ICS)**: A standardized approach to the command, control, and coordination of on-scene incident management, providing a common hierarchy within which personnel from multiple organizations may be effective. ICS is the combination of procedures, personnel, facilities, equipment, and communications operating within a common organizational structure, designed to aid in the management of on-scene resources during incidents. It is used for all kinds of incidents and is applicable to small, as well as large and complex, incidents, including planned events.

- **Industrial Control System (ICS)**: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets. It is also known as operational technology.

- **Information Technology (IT)**: Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

- **Insider Threat**: A person or group of persons within an organization who pose a potential risk through violating security policies. One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that enabling them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

- **Integrity**: The property whereby information, an information system or a component of a system has not been modified or destroyed in an unauthorized manner. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

- **Malware**: Software that compromises the operation of a system by performing an unauthorized function or process. Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that has adverse impacts on the confidentiality, integrity, or availability of an information system.

- **Mitigation**: The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

- **Network Services**: Firewalls, including relevant hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

- **Operational Technology (OT)**: The hardware and software systems used to operate industrial control devices.

- **Phishing**: A digital form of social engineering to deceive individuals into providing sensitive information, including usernames and passwords.

- **Privacy**: The assurance that the confidentiality of, and access to, certain information about an entity is protected.

- **Recovery**: The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

- **Resilience**: The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

- **Service**: A resource or capability provided by an asset that may be used for operational or information functions.

- **Significant Cyber Incident**: A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

- **Spyware**: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

- **System**: A combination of interacting elements organized to achieve one or more stated purposes. Interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. Source: NIST SP 800-160 Vol. 2 Rev. 1.

- **Trojan:** A computer program that appears to be useful by evading security mechanisms, but aims to harm a system or steal information, sometimes through exploiting legitimate authorizations of a system entity invoking the program.

- **Unauthorized Access**: Any access that violates the stated security policy.

- **Upstream Dependencies:** These are products or services provided to a jurisdiction by an external organization that are necessary to support its operations and functions.

- **Worm:** A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Appendix E: Acronyms

BOD	Binding Operational Directive
CDT	Cyber Disruption Team
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CPG	Comprehensive Preparedness Guide
CRR	Cyber Resilience Review
CSET	Cyber Security Evaluation Tool
CRRA	Cyber Response and Recovery Act
CRRF	Cyber Response and Recovery Fund
CTO	Chief Technology Officer
DHS	Department of Homeland Security
DOS	Denial of Service
EOP	Emergency Operations Plan
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Industrial Control Systems OR Incident Command System
ISAC	Information Sharing & Analysis Center
IT	Information Technology
KEV	Known Exploited Vulnerability

NCIRP	National Cyber Incident Response Plan
NCSR	Nationwide Cybersecurity Review
NDA	Non-Disclosure Agreement
NECP	National Emergency Communications Plan
NIMS	National Incident Management System
NIST	National Institute of Science and Technology
OT	Operational Technology
PACE	Primary, Alternate, Contingency, and Emergency
PII	Personally Identifiable Information
PISCES	Public Infrastructure Security Cyber Education System
PSA	Protective Security Advisor
SLTT	State, Local, Tribal, and Territorial
THIRA	Threat and Hazard Identification and Risk Assessment
TSP	Telecommunications Service Priority
TTP	Tactics, Techniques, and Procedures
UCG	Unified Coordination Group
WPS	Wireless Priority Service

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

#StopRansomware Guide

Publication: October 2023

Disclaimer: *This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.*

Change Record

Version	Date	Revision/Change Description	Section/Page Affected
1.0	September 2020	Initial Version	
2.0	May 2023	See “What’s New” on p.3.	Updates throughout.
3.0	October 2023	• Initial Access Vector bullet added for internet-facing vulnerabilities. • Updated guidance on hardening SMB. • Added information about threat actors impersonating employees. • Added guidance on hardening web browsers. • Added a bullet about abnormal amounts of data outgoing over any ports. • Added Acknowledgements section.	• Initial Access Vector: Internet-Facing Vulnerabilities and Mitigations p.7. • Part 1: Ransomware and Data Extortion Preparation, Prevention, and Mitigation Best Practices, pages 8, and 9. • Initial Access Vector: Advanced Forms of Social Engineering p.14. • General Best Practices and Hardening Guidance, p.20. • Part 2: Ransomware and Data Extortion Response Checklist p. 24. • Acknowledgements, p.30.

INTRODUCTION

Ransomware is a form of malware designed to encrypt files on a device, rendering them and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Over time, malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim data and pressured victims to pay by threatening to release the stolen data. The application of both tactics is known as "double extortion." In some cases, malicious actors may exfiltrate data and threaten to release it as their sole form of extortion without employing ransomware.

These ransomware and associated data breach incidents can severely impact business processes by leaving organizations unable to access necessary data to operate and deliver mission-critical services. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery.

This guide is an update to the Joint Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing & Analysis Center (MS-ISAC) Ransomware Guide released in September 2020 (see What's New) and was developed through the JRTF. This guide includes two primary resources:

- Part 1: Ransomware and Data Extortion Prevention Best Practices
- Part 2: Ransomware and Data Extortion Response Checklist

Part 1 provides guidance for all organizations to reduce the impact and likelihood of ransomware incidents and data extortion, including best practices to prepare for, prevent, and mitigate these incidents. Prevention best practices are grouped by common initial access vectors. Part 2 includes a checklist of best practices for responding to these incidents.

These ransomware and data extortion prevention and response best practices and recommendations are based on operational insight from CISA, MS-ISAC, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), hereafter referred to as the authoring organizations. The

This guide was developed through the U.S. Joint Ransomware Task Force (JRTF).

The JRTF, co-chaired by CISA and FBI, is an interagency, collaborative effort to combat the growing threat of ransomware attacks. The JRTF was launched in response to a series of high-profile ransomware attacks on U.S. critical infrastructure and government agencies. The JRTF:

1. Coordinates and streamlines the U.S. Government's response to ransomware attacks and facilitates information sharing and collaboration between government agencies and private sector partners.
2. Ensures operational coordination for activities such as developing and sharing best practices for preventing and responding to ransomware attacks, conducting joint investigations and operations against ransomware threat actors, and providing guidance and resources to organizations that have been victimized by ransomware.
3. Represents a significant step forward in enabling unity of effort across the U.S Government's efforts to address the growing threat of ransomware attacks.

For more info on JRTF, see cisa.gov/joint-ransomware-task-force.

audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

The authoring organizations recommend that organizations take the following initial steps to prepare and protect their facilities, personnel, and customers from cyber and physical security threats and other hazards:

- Join a sector-based information sharing and analysis center (ISAC), where eligible, such as:
    - MS-ISAC for U.S. State, Local, Tribal, & Territorial (SLTT) Government Entities - learn.cisecurity.org/ms-isac-registration. MS-ISAC membership is open to representatives from all 50 states, the District of Columbia, U.S. Territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the United States.
    - Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) for U.S. Elections Organizations - learn.cisecurity.org/ei-isac-registration. See the National Council of ISACs for more information.
- Contact CISA at CISA.JCDC@cisa.dhs.gov to collaborate on information sharing, best practices, assessments, exercises, and more.
- Contact your local FBI field office for a list of points of contact (POCs) in the event of a cyber incident.

Engaging with peer organizations and CISA enables your organization to receive critical and timely information and access to services for managing ransomware and other cyber threats.

What's New

Since the initial release of the Ransomware Guide in September 2020, ransomware actors have accelerated their tactics and techniques.

To maintain relevancy, add perspective, and maximize the effectiveness of this guide, the following changes have been made:

- Incorporated the #StopRansomware effort into the title.
- Added recommendations for preventing common initial infection vectors, including compromised credentials and advanced forms of social engineering.
- Updated recommendations to address cloud backups and zero trust architecture (ZTA).
- Expanded the ransomware response checklist with threat hunting tips for detection and analysis.
- Mapped recommendations to CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).

#StopRansomware is CISA and FBI's effort to publish advisories for network defenders that detail network defense information related to various ransomware variants and threat actors. Visit stopransomware.gov to learn more and to read the joint advisories.

Part 1: Ransomware and Data Extortion Preparation, Prevention, and Mitigation Best Practices

These recommended best practices align with the CPGs developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. For more information on the CPGs and recommended baseline protections, visit CISA's Cross-Sector Cybersecurity Performance Goals.

Preparing for Ransomware and Data Extortion Incidents

Refer to the best practices and references listed in this section to help manage the risks posed by ransomware and to drive a coordinated and efficient response for your organization in the event of an incident. Apply these practices to the greatest extent possible pending the availability of organizational resources.

- **Maintain offline, encrypted backups of critical data**, and regularly test the availability and integrity of backups in a disaster recovery scenario [CPG 2.R]. Test backup procedures on a regular basis. It is important that backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.
    - Maintain and regularly update "golden images" of critical systems. This includes maintaining image "templates" that have a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server [CPG 2.O].
        - Use infrastructure-as-code (IaC) to deploy and update cloud resources and keep backups of template files offline to quickly redeploy resources. IaC code should be version controlled and changes to the templates should be audited.
        - Store applicable source code or executables with offline backups (as well as escrowed and license agreements). Rebuilding from system images is more efficient, but some images will not install on different hardware or platforms correctly; having separate access to software helps in these cases.

> Automated cloud backups may not be sufficient because if local files are encrypted by an attacker, these files will be synced to the cloud, possibly overwriting unaffected data.

  - Retain backup hardware to rebuild systems if rebuilding the primary system is not preferred.
    - Consider replacing out-of-date hardware that inhibits restoration with up-to-date hardware, as older hardware can present installation or compatibility hurdles when rebuilding from images.
  - Consider using a multi-cloud solution to avoid vendor lock-in for cloud-to-cloud backups in case all accounts under the same vendor are impacted.
    - Some cloud vendors offer immutable storage solutions that can protect stored data without the need for a separate environment. Use immutable storage with caution as it does not meet compliance criteria for certain regulations and misconfiguration can impose significant cost.

- **Create, maintain, and regularly exercise a basic cyber incident response plan (IRP) and associated communications plan that includes response and notification procedures** for ransomware and data extortion/breach incidents [CPG 2.S]. Ensure a hard copy of the plan and an offline version is available.
  - Provide data breach notifications to third parties and regulators consistent with law.
  - Ensure the IRP and communications plan are reviewed and approved by the CEO, or equivalent, in writing and that both are reviewed and understood across the chain of command.
  - Review available incident response guidance, such as the Ransomware Response Checklist in this guide and Public Power Cyber Incident Response Playbook to:
    - Help your organization better organize around cyber incident response.
    - Draft cyber incident holding statements.
    - Develop a cyber IRP.
  - Include organizational communications procedures as well as templates for cyber incident holding statements in the communications plan. Reach a consensus on what level of detail is appropriate to share within the organization and with the public and how information will flow.

- **Implement a zero trust architecture** to prevent unauthorized access to data and services. Make access control enforcement as granular as possible. ZTA assumes a network is compromised and provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per request access decisions in information systems and services.

Preventing and Mitigating Ransomware and Data Extortion Incidents

Refer to the best practices and references listed in this section to help prevent and mitigate ransomware and data extortion incidents. Prevention best practices are grouped by common initial access vectors of ransomware and data extortion actors.

Initial Access Vector: Internet-Facing Vulnerabilities and Misconfigurations

- **Do not expose services, such as remote desktop protocol, on the web**. If these services must be exposed, apply appropriate compensating controls to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets. [CPG 2.W]
- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface [CPG 1.E].
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: cisa.gov/cyber-resource-hub [CPG 1.F].
- **Regularly patch and update software and operating systems to the latest available versions**.
  - Prioritize timely patching of internet-facing servers—that operate software for processing internet data, such as web browsers, browser plugins, and document readers—especially for known exploited vulnerabilities.
  - The authoring organizations—aware of difficulties small and medium business have keeping internet-facing servers updated—urge migrating systems to reputable "managed" cloud providers to reduce, not eliminate, system maintenance roles for identity and email systems. For more information, visit NSA's Cybersecurity Information page Mitigating Cloud Vulnerabilities.
- **Ensure all on-premises, cloud services, mobile, and personal (i.e., bring your own device [BYOD]) devices are properly configured and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes (e.g., Remote Desktop Protocol [RDP]—Transmission Control Protocol [TCP] Port 3389) [CPG 2.X].
  - Reduce or eliminate manual deployments and codify cloud resource configuration through IaC. Test IaC templates before deployment with static security scanning tools to identify misconfigurations and security gaps.
  - Check for configuration drift routinely to identify resources that were changed or introduced outside of template deployment, reducing the likelihood of new security gaps and misconfigurations being introduced. Leverage cloud providers' services to automate or facilitate auditing resources to ensure a consistent baseline.
- **Limit the use of RDP and other remote desktop services**. If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client. Threat actors also often gain access by exploiting virtual private networks (VPNs) or using compromised credentials. Refer to CISA Advisory: Enterprise VPN Security.
  - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multifactor authentication (MFA), and log RDP login attempts.
  - Update VPNs, network infrastructure devices, and devices being used to remote in to work environments with the latest software patches and security configurations.

  - Implement MFA on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use passwords of 15 or more characters.

- Disable Server Message Block (SMB) protocol version 1 and upgrade to version 3 (SMBv3) after mitigating existing dependencies (on existing systems or applications), as they may break when disabled. SMBv3 was first released as part of updates to Microsoft Windows 8 and Windows Server 2012, Apple OS X 10.10, and Linux kernel 3.12.
- Harden SMBv3 by implementing the following guidance as malicious actors use SMB to propagate malware across organizations.
  - Require the use of SMBv 3.1.1. This version contains enhanced security protections, including pre-authentication integrity, enhanced AES encryption, and signing cryptography. SMBv 3.1.1 protocol is supported natively in Windows, Apple, and Linux kernel, as well as many other third-party storage systems. In Microsoft Windows 10 and Windows Server 2019, Windows 11 Preview Build 25951, and later, you can mandate SMBv 3.1.1 protections such as dialect client negotiation. For more information, see Microsoft's Protect SMB traffic from interception | Use SMB 3.1.1 and SMB dialect management now supported in Windows Insider.
  - Block unnecessary SMB communications:
    - Block external access of SMB to and from organization networks by blocking TCP port 445 inbound and outbound at internet perimeter firewalls. Block TCP ports 137, 138, 139. **Note:** SMBv2 and later does not use NetBIOS datagrams. Continuing to use SMBv2 does not have significant risks and can be used where needed. It is recommended to update it to SMBv3 where feasible.
    - Block or limit internal SMB traffic so that communications only occur between systems requiring it. For instance, Windows devices need SMB communications with domain controllers to get group policy, but most Windows workstations do not need to access other Windows workstations.
    - Configure Microsoft Windows and Windows Server systems to require Kerberos-based IP Security (IPsec) for lateral SMB communications to prevent malicious actors from accessing communications over SMB by detecting systems that are not members of an organization's Microsoft Active Directory domains.
    - Disable the SMB Server service ("Server") on Microsoft Windows and Windows Server devices in instances where there is no need to remotely access files or to name pipe application programming interfaces (APIs).
    - For more information guidance, see Microsoft's Secure SMB Traffic in Windows Server.
  - Consider requiring SMB encryption. To guarantee that SMB 3.1.1 clients always use SMB Encryption, you must disable the SMB 1.0 server. For more information, refer to Microsoft's SMB security enhancements | Enable SMB Encryption and Reduced performance after SMB Encryption or SMB Signing is enabled
  - If SMB encryption is not enabled, require SMB signing for both SMB client and server on all systems. This will prevent certain adversary-in-the-middle and pass-the-hash attacks.

  For more information on SMB signing, refer to Microsoft's Overview of Server Message Block Signing.
  - Require Kerberos authentication by hardening Universal Naming Convention (UNC). OSs such as Microsoft Windows 10, Windows Server 2016, and later automatically harden UNC for connections to the Microsoft Active Directory domain via SYSVOL and NETLOGON shares. Additionally, network administrators can manually configure UNC hardening for servers and shares in any supported Microsoft Windows operating system. For more information, refer to Microsoft's Vulnerability in Group Policy could allow remote code execution. Using IP addresses to connect to SMB servers will result in the use of NTLM authentication unless you also configure the use of Kerberos SPNs with IP addresses, refer to Microsoft's Configuring Kerberos for IP Address.
  - Use SMB over QUIC. Microsoft Windows 11, Windows Server 2022 Datacenter: Azure Edition, and Android clients with a third-party SMB client support use of SMB over QUIC, an alternative for SMB over TCP. The QUIC protocol is always Transport Layer Security (TLS) 1.3 encrypted and uses certificate authentication to encapsulate all SMB traffic—including SMB's own authentication—inside a VPN-like transport. SMB over QUIC allows mobile users to safely connect over the public internet to edge SMB resources, such as servers at the edge of organizational networks not completely behind a firewall, but also works on internal networks that require the highest SMB transport security. For more information, refer to Microsoft's SMB over QUIC.
  - Log and monitor SMB traffic [CPG 2.T] to help flag potentially abnormal, harmful behaviors.

Initial Access Vector: Compromised Credentials

- **Implement phishing-resistant MFA for all services**, particularly for email, VPNs, and accounts that access critical systems [CPG 2.H]. Escalate to senior management upon discovery of systems that do not allow MFA, systems that do not enforce MFA, and any users who are not enrolled with MFA.
  - **Consider employing password-less MFA** that replace passwords with two or more verification factors (e.g., a fingerprint, facial recognition, device pin, or a cryptographic key).
- **Consider subscribing to credential monitoring services** that monitor the dark web for compromised credentials.
- **Implement identity and access management (IAM) systems** to provide administrators with the tools and technologies to monitor and manage roles and access privileges of individual network entities for on-premises and cloud applications.
- **Implement zero trust access control** by creating strong access policies to restrict user to resource access and resource-to-resource access. This is important for key management resources in the cloud.
- **Change default admin usernames and passwords** [CPG 2.A].
- **Do not use root access accounts for day-to-day operations**. Create users, groups, and roles to carry out tasks.

- **Implement password policies that require unique passwords of at least 15 characters**. [CPG 2.B] [CPG 2.C].
    - Password managers can help you develop and manage secure passwords. Secure and limit access to any password managers in use and enable all security features available on the product in use, such as MFA.
- **Enforce account lockout policies after a certain number of failed login attempts**. Log and monitor login attempts for brute force password cracking and password spraying [CPG 2.G].
- **Store passwords in a secured database and use strong hashing algorithms**.
- **Disable saving passwords to the browser in the Group Policy Management console**.
- **Implement Local Administrator Password Solution (LAPS)** where possible if your OS is older than Windows Server 2019 and Windows 10 as these versions do not have LAPS built in. **Note:** The authoring organizations recommend organizations upgrade to Windows Server 2019 and Windows 10 or greater.
- Protect against Local Security Authority Subsystem Service (LSASS) dumping:
    - **Implement the Attack Surface Reduction (ASR) rule for LSASS.**
    - **Implement Credential Guard for Windows 10 and Server 2016**. Refer to Microsoft Manage Windows Defender Credential Guard for more information. For Windows Server 2012R2, enable Protected Process Light (PPL) for Local Security Authority (LSA).
- **Educate all employees on proper password security in your annual security training** to include emphasizing not reusing passwords and not saving passwords in local files.
- **Use Windows PowerShell Remoting, Remote Credential Guard, or RDP** with restricted Admin Mode as feasible when establishing a remote connection to avoid direct exposure of credentials.
- **Separate administrator accounts from user accounts** [CPG 2.E]. Only allow designated admin accounts to be used for admin purposes. If an individual user needs administrative rights over their workstation, use a separate account that does not have administrative access to other hosts, such as servers. For some cloud environments, separate duties when the account used to provision/manage keys does not have permission to use the keys and vice versa. As this strategy introduces additional management overhead, it is not appropriate in all environments.

Initial Access Vector: Phishing

- **Implement a cybersecurity user awareness and training program** that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents [CPG 2.I].
- **Implement flagging external emails in email clients**.
- **Implement filters at the email gateway to filter out emails** with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall [CPG 2.M].

CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments. Visit cisa.gov/cyber-resource-hub.

- **Enable common attachment filters to restrict file types that commonly contain malware** and should not be sent by email. For more information, refer to Microsoft's post Anti-malware protection in EOP.
    - Review file types in your filter list at least semi-annually and add additional file types that have become attack vectors. For example, OneNote attachments with embedded malware have recently been used in phishing campaigns.
    - Malware is often compressed in password protected archives that evade antivirus scanning and email filters.
- **Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification** to lower the chance of spoofed or modified emails from valid domains. DMARC protects your domain from being spoofed but does not protect from incoming emails that have been spoofed unless the sending domain also implements DMARC. DMARC builds on the widely deployed Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email. For more information on DMARC, refer to CISA Insights Enhance Email & Web Security and the Center for Internet Security's blog How DMARC Advances Email Security.

Malicious Domain Blocking and Reporting (MDBR) is a no-cost service for SLTT organizations that is funded by CISA, the MS-ISAC, and the EI-ISAC. This fully managed security service prevents IT systems from connecting to harmful web domains and protects against cyber threats, including:

- Malware,
- Ransomware, and
- Phishing.

To sign up for MDBR, visit cisecurity.org/ms-isac/services/mdbr/.

- **Ensure macro scripts are disabled for Microsoft Office files transmitted via email**. These macros can be used to deliver ransomware [CPG 2.N]. **Note:** Recent versions of Office are configured by default to block files that contain Visual Basic for Applications (VBA) macros and display a Trust Bar with a warning that macros are present and have been disabled. For more information, refer to Microsoft's Macros from the internet will be blocked by default in Office. See Microsoft's Block macros from running in Office files from the Internet for configuration instructions to disable macros in external files for earlier versions of Office.
- **Disable Windows Script Host (WSH)**. Windows script hosting provides an environment in which users can execute scripts or perform tasks.

Initial Access Vector: Precursor Malware Infection

CISA and MS-ISAC encourage SLTT organizations to use Albert IDS to enhance a defense-in-depth strategy. Albert serves as an early warning capability for U.S. SLTT governments and supports nationwide cybersecurity situational awareness and defense. For more information regarding Albert, visit cisecurity.org/services/albert-network-monitoring/.

- **Use automatic updates for your antivirus and anti-malware software and signatures**. Ensure tools are properly configured to escalate warnings and indicators to notify security personnel. The authoring organizations recommend using a centrally managed antivirus solution. This enables detection of both “precursor” malware and ransomware.
    - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as QakBot, Bumblebee, and Emotet.
    - In some cases, ransomware deployment is the last step in a network compromise and is dropped to obscure previous post-compromise activities, such as business email compromise (BEC).
- **Use application allowlisting and/or endpoint detection and response (EDR) solutions** on all assets to ensure that only authorized software is executable and all unauthorized software is blocked.
    - For Windows, enable Windows Defender Application Control (WDAC), AppLocker, or both on all systems that support these features.
        - WDAC is under continuous development while AppLocker will only receive security fixes. AppLocker can be used as a complement to WDAC, when WDAC is set to the most restrictive level possible, and AppLocker is used to fine-tune restrictions for your organization.
    - Use allowlisting rather than attempting to list and deny every possible permutation of applications in a network environment.
    - Consider implementing EDR for cloud-based resources.
- **Consider implementing an intrusion detection system (IDS)** to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.
    - Ensure that the IDS is centrally monitored and managed. Properly configure the tools and route warnings and indicators to the appropriate personnel for action.
- **Monitor indicators of activity and block malware file creation with the Windows Sysmon utility**. As of Sysmon 14, the `FileBlockExecutable` option can be used to block the creation of malicious executables, Dynamic Link Library (DLL) files, and system files that match specific hash values.

Initial Access Vector: Advanced Forms of Social Engineering

- **Create policies to include cybersecurity awareness training** about advanced forms of social engineering for personnel that have access to your network. Training should include tips on being able to recognize illegitimate websites and search results. It is also important to repeat security awareness training regularly to keep your staff informed and vigilant.
- **Implement Protective Domain Name System (DNS).** By blocking malicious internet activity at the source, Protective DNS services can provide high network security for remote workers. These security services analyze DNS queries and take action to mitigate threats—such as malware, ransomware, phishing attacks, viruses, malicious sites, and spyware—leveraging the existing DNS protocol and architecture. SLTT's can implement the no-cost MDBR service. See NSA's and CISA's Selecting a Protective DNS Service.
- **Consider implementing sandboxed browsers** to protect systems from malware originating from web browsing. Sandboxed browsers isolate the host machine from malicious code.

Advanced forms of social engineering include:

- Search Engine Optimization (SEO) poisoning, also known as search poisoning: When malicious actors create malicious websites and use SEO tactics to make them show up prominently in search results. SEO poisoning hijacks the search engine results of popular websites and injects malicious links to boost their placement in search results. These links then lead unsuspecting users to phishing sites, malware downloads, and other cyber threats.
- Drive-by-downloads (imposter websites): When a user unintentionally downloads malicious code by visiting a seemingly legitimate website that is malicious. Malicious actors use drive-by downloads to steal and collect personal information, inject trojans, or introduce exploit kits or other malware to endpoints. Users may visit these sites by responding to a phishing email or by clicking on a deceptive pop-up window.
- "Malvertising": Malicious advertising that cybercriminals use to inject malware to users' computers when they visit malicious websites or click an online advertisement. Malvertising may also direct users to a corrupted website where their data can be stolen, or malware can be downloaded onto their computer. Malvertising can appear anywhere, even at sites you visit as part of your everyday web browsing.
- Impersonating employees: Ransomware actors have posed as company IT and/or helpdesk staff in phone calls or SMS messages to obtain credentials from employees and gain access to the network.

Initial Access Vector: Third Parties and Managed Service Providers

- **Consider the risk management and cyber hygiene practices of third parties or managed service providers (MSPs)** your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting numerous client organizations [CPG 1.I].
    - If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they are following the applicable best practices outlined above. Use contract language to formalize your security requirements as a best practice.

Malicious actors may exploit the trusted relationships your organization has with third parties and MSPs.

- Malicious actors may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.
- Malicious actors may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with to phish your users, enabling network compromise and disclosure of information.

- **Ensure the use of least privilege and separation of duties when setting up the access of third parties**. Third parties and MSPs should only have access to devices and servers that are within their role or responsibilities.
- **Consider creating service control policies (SCP) for cloud-based resources to prevent users or roles, organization wide, from being able to access specific services or take specific actions within services.** For example, the SCP can be used to restrict users from being able to delete logs, update virtual private cloud (VPC) configurations, and change log configurations.

General Best Practices and Hardening Guidance

- **Ensure your organization has a comprehensive asset management** approach [CPG 1.A].
    - Understand and take inventory of your organization's IT assets, logical (e.g., data, software) and physical (e.g., hardware).
    - Know which data or systems are most critical for health and safety, revenue generation, or other critical services, and understand any associated interdependencies (e.g., "system list 'A' used to perform 'X' is stored in critical asset 'B'"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
    - Ensure you store your IT asset documentation securely and keep offline backups and physical hard copies on site.

Tip: To facilitate asset tracking, use MS-ISAC's Hardware and Software Asset Tracking Spreadsheet.

- **Apply the principle of least privilege to all systems and services** so that users only have the access they need to perform their jobs [CPG 2.E]. Malicious actors often leverage privileged accounts for network-wide ransomware attacks.
    - Restrict user permissions to install and run software applications.
    - Restrict user/role permissions to access or modify cloud-based resources.
    - Limit actions that can be taken on customer-managed keys by certain users/roles.
    - Block local accounts from remote access by using group policy to restrict network sign-in by local accounts. For guidance, refer to Microsoft's Blocking Remote Use of Local Accounts and Security identifiers.
    - Use Windows Defender Remote Credential Guard and restricted admin mode for RDP sessions.
    - Remove unnecessary accounts and groups and restrict root access.
    - Control and limit local administration.
    - Audit Active Directory (AD) for excessive privileges on accounts and group memberships.
    - Make use of the Protected Users AD group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
    - Audit user and admin accounts for inactive or unauthorized accounts quarterly. Prioritize review of remote monitoring and management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.

- **Ensure that all hypervisors and associated IT infrastructure, including network and storage components, are updated and hardened**. Emerging ransomware strategies have begun targeting VMware ESXi servers, hypervisors, and other centralized tools and systems, which enables fast encryption of the infrastructure at scale. For more information about ransomware resilience and hardening of VMware and other virtualization infrastructure, see:
    - NIST Special Publication (SP 800-125A Rev.1): Security Recommendations for Server-based Hypervisor Platforms
    - VMware: Cloud Infrastructure Security Configuration & Hardening

- **Leverage best practices and enable security settings in association with cloud environments**, such as Microsoft Office 365.
    - Review the shared responsibility model for cloud and ensure you understand what makes up customer responsibility when it comes to asset protection.
    - Backup data often; offline or leverage cloud-to-cloud backups.
    - Enable logging on all resources and set alerts for abnormal usages.
    - Enable delete protection or object lock on storage resources often targeted in ransomware attacks (e.g., object storage, database storage, file storage, and block storage) to prevent data from being deleted or overwritten, respectively.
    - Consider enabling version control to keep multiple variants of objects in storage. This allows for easier recovery from unintended or malicious actions.

  - Where supported, when using custom programmatic access to the cloud, use signed application programming interface (API) requests to verify the identity of the requester, protect data in transit, and protect against other attacks such as replay attacks.
  - For more information, refer to CISA Cybersecurity Advisory Microsoft Office 365 Security Recommendations.

- **Mitigate the malicious use of remote access and remote monitoring and management (RMM)** software:
  - Audit remote access tools on your network to identify current or authorized RMM software.
  - Review logs for execution of RMM software to detect abnormal use, or RMM software running as a portable executable.
  - Use security software to detect instances of RMM software only being loaded in memory.
  - Require authorized RMM solutions only be used from within your network over approved remote access solutions, such as VPNs or virtual desktop interfaces (VDIs).
  - Block both inbound and outbound connections on common RMM ports and protocols at the network perimeter.

- **Employ logical or physical means of network segmentation by implementing** ZTA and separating various business units or departmental IT resources within your organization and maintain separation between IT and operational technology [CPG 2.F]. Network segmentation can help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. Organizations should use due diligence when segmenting networks and ensure network security policies are in place and adhered to because segmentation can be rendered ineffective if it is breached through user error or non-adherence to policies (e.g., connecting removable storage media or other devices to multiple segments).

- **Develop and regularly update comprehensive network diagram(s) that describes systems and data flows within your organization's network(s)** (see Figure 1) [CPG 2.P]. This is useful in steady state and can help incident responders understand where to focus their efforts. See Figure 2 and Figure 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.
  - The diagram should include depictions of major networks, any specific IP addressing schemes, and the general network topology including network connections, interdependencies, and access granted to third parties, MSPs, and cloud connections from external and internal endpoints.
  - Ensure you securely store network documentation and keep offline backups and hard copies on site.

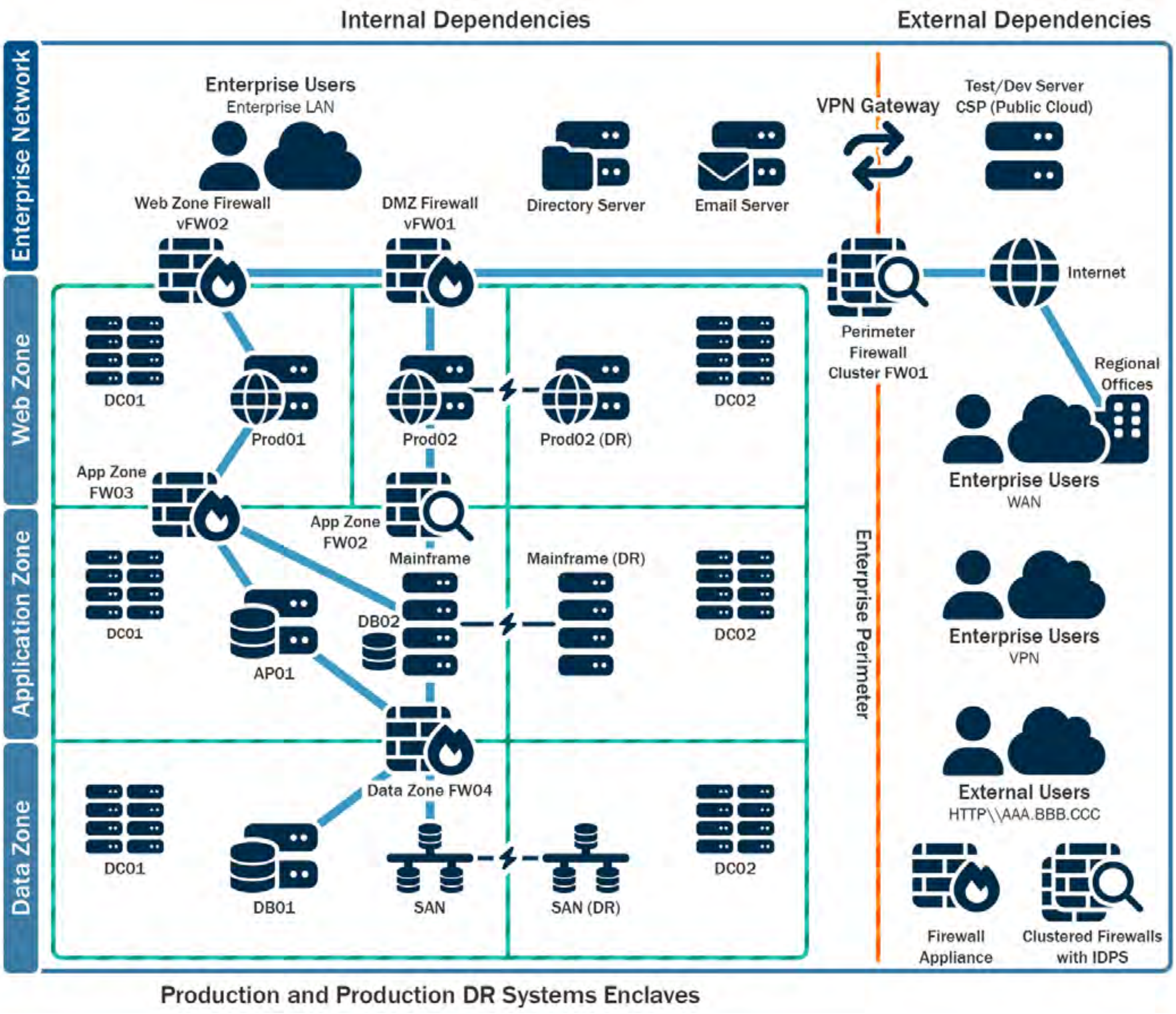


Figure 1: Example Network Diagram

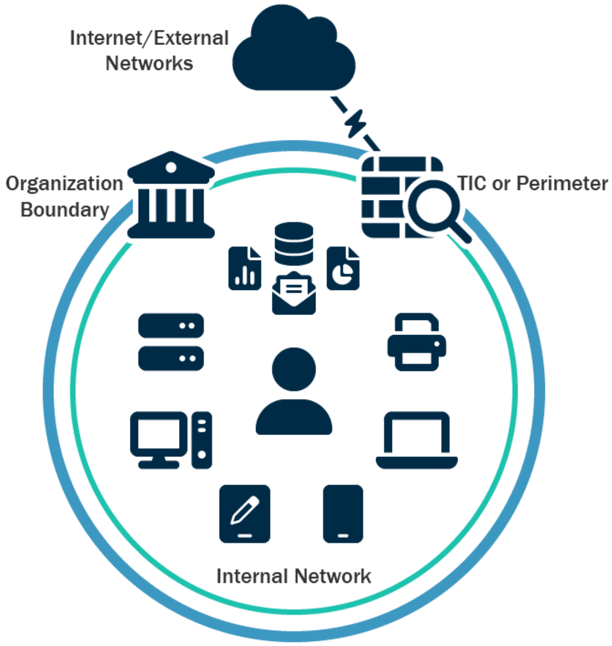


Figure 2: Flat (Unsegmented) Network

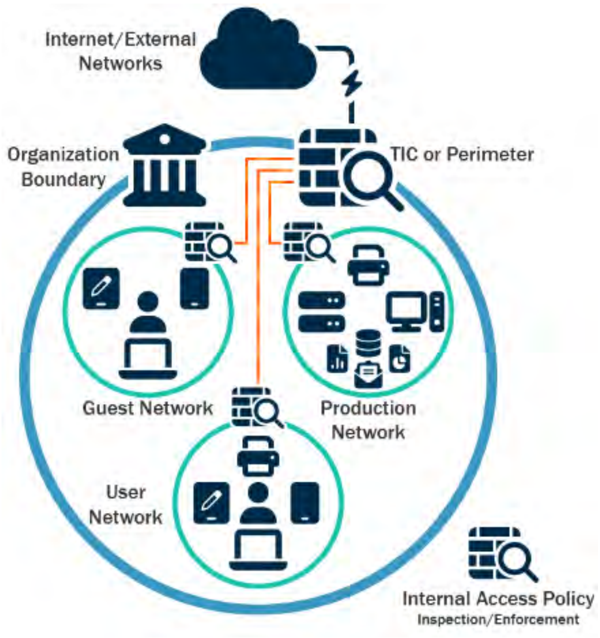


Figure 3: Segmented Network

- **Restrict usage of PowerShell to specific users on a case-by-case basis by using Group Policy**. Typically, only users or administrators who manage a network or Windows OS are permitted to use PowerShell. PowerShell is a cross-platform, command-line, shell, and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities. For more information, refer to the joint Cybersecurity Information Sheet Keeping PowerShell: Security Measure to Use and Embrace.
  - Update Windows PowerShell or PowerShell Core to the latest version and uninstall all earlier PowerShell versions.
  - Ensure PowerShell instances, using the most current version, have module, script block, and transcription logging enabled (enhanced logging).
    - Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
    - Two logs that record PowerShell activity are the "PowerShell Windows Event" log and the "PowerShell Operational" log. The authoring organizations recommend turning on these two Windows Event Logs with a retention period of at least 180 days.
    - These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

- **Secure domain controllers (DCs)**. Malicious actors often target and use DCs as a staging point to spread ransomware network wide. To secure DCs:
  - Use the latest version of Windows Server supported by your organization on DCs. Newer versions of Windows Server OS have more security features, including for Active Directory, integrated. For guidance on configuring available security features refer to Microsoft's Best Practices for Securing Active Directory.
    - The authoring organizations recommend using Windows Server 2019 or greater and Windows 10 or greater as they have security features, such as LSASS protections with Windows Credential Guard, Windows Defender, and Antimalware Scan Interface (AMSI), not included in older operating system
  - Ensure that DCs are regularly patched. Apply patches for critical vulnerabilities as soon as possible.
  - Use open-source penetration testing tools, such as BloodHound or PingCastle, to verify domain controller security.
  - Ensure that minimal software or agents are installed on DCs because these can be leveraged to run arbitrary code on the system.
  - Restrict access to DCs to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions. For more information, refer to Microsoft's Securing Active Directory Administrative Groups and Accounts.
    - The designated admin accounts should only be used for admin purposes. Ensure that checking emails, web browsing, or other high-risk activities are not performed on DCs.
  - Configure DC host firewalls to prevent internet access. Usually, DCs do not need direct internet access. Servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
  - Implement a privileged access management (PAM) solution on DCs to assist in managing and monitoring privileged access. PAM solutions can also log and alert usage to detect unusual activity.
  - Consider disabling or limiting NTLM and WDigest Authentication, if possible. Include their use as criteria for prioritizing upgrading legacy systems or for segmenting the network. Instead use modern federation protocols (e.g., SAML, OIDC or Kerberos) for authentication with AES-256 bit encryptionhttps://cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf. If NTLM must be enabled:
    - Enable Extended Protection for Authentication (EPA) to prevent some NTLM-relay attacks. For more information, refer to Microsoft Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS).
    - Enable NTLM auditing to ensure that only NTLMv2 responses are sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.

  - Enable additional protections for LSA Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against `lsass.exe` to ensure an understanding of the programs that will be affected by the enabling of this protection.

- **Retain and adequately secure logs from network devices, local hosts, and cloud services**. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain if an incident has occurred [CPG 2.T].
  - Set up centralized log management using a security information and event management tool [CPG 2.U]. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can triage an individual event and determine its impact to the organization.
  - Maintain and back up logs for critical systems for a minimum of one year, if possible.

- **Establish a security baseline of normal network traffic and tune network appliances to detect anomalous behavior**. Tune host-based products to detect anomalous binaries, lateral movement, and persistence techniques.
  - Consider using business transaction logging—such as logging activity related to specific or critical applications—for behavioral analytics.

- **Conduct regular assessments** to ensure processes and procedures are up to date and can be followed by security staff and end users.
- **Enable tracking prevention** to limit the vectors that ad networks and trackers can use to track user information.
- **Enable website typo protection** to limit the possibility of logging onto spoofed websites or other potential malicious links that could compromise a browser.
- **Enable browser-based AV** for active scanning while browsing as an added layer of defense.
- **Block website notifications by default** to limit site's ability to track user data that can be exploited.

Part 2: Ransomware and Data Extortion Response Checklist

Should your organization be a victim of ransomware, follow your approved IRP. The authoring organizations strongly recommend responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

The authoring organizations do not recommend paying ransom. Paying ransom will not ensure your data is decrypted, that your systems or data will no longer be compromised, or that your data will not be leaked.

Additionally, paying ransoms may pose sanctions risks. For information on potential sanctions risks, see U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) memorandum from September 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The updated advisory states that Treasury's Office of Foreign Assets Control (OFAC) would consider 'mitigating factors' in related enforcement actions. Contact your local FBI field office, in consultation with OFAC, for guidance on mitigating penalty factors after an attack.

Detection and Analysis

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- ☐ **1. Determine which systems were impacted, and immediately isolate them.**
  - ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
  - ☐ Prioritize isolating critical systems that are essential to daily operations.
  - ☐ If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
  - ☐ For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigation.
  - ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access or deploy ransomware widely prior to networks being taken offline.

- ☐ **2. Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.**

  Note: This step will prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. **It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network** using other means.

☐ **3. Triage impacted systems for restoration and recovery.**

- ☐ Identify and prioritize critical systems for restoration on a clean network and confirm the nature of data housed on impacted systems.
  - ▪ Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ **4. Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) and logs.** Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

- ☐ Look for evidence of precursor “dropper” malware, such as Bumblebee, Dridex, Emotet, QakBot, or Anchor. A ransomware event may be evidence of a previous, unresolved network compromise.
  - ▪ Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network to further extort the victim and pressure them into paying.
  - ▪ Malicious actors often drop ransomware variants to obscure post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromises.

☐ **5. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**

☐ **6. Initiate threat hunting activities.**

- ☐ For enterprise environments, check for:
  - ▪ Newly created AD accounts or accounts with escalated privileges and recent activity related to privileged accounts such as Domain Admins.
  - ▪ Anomalous VPN device logins or other suspicious logins.
  - ▪ Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations. Look for anomalous usage of built-in Windows tools such as `bcdedit.exe`, `fsutil.exe` (deletejournal), `vssadmin.exe`, `wbadmin.exe`, and `wmic.exe` (shadowcopy or shadowstorage). Misuse of these tools is a common ransomware technique to inhibit system recovery.
  - ▪ Signs of the presence of Cobalt Strike beacon/client. Cobalt Strike is a commercial penetration testing software suite. Malicious actors often name Cobalt Strike Windows processes with the same names as legitimate Windows processes to obfuscate their presence and complicate investigations.

- Signs of any unexpected usage of remote monitoring and management (RMM) software (including portable executables that are not installed). RMM software is commonly used by malicious actors to maintain persistence.
- Any unexpected PowerShell execution or use of PsTools suite.
- Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz, `Sysinternals ProcDump`, or `NTDSutil.exe`).
- Signs of unexpected endpoint-to-endpoint (including servers) communications, for example, Address Resolution Protocol (ARP) poisoning of an endpoint or command and control traffic relayed between endpoints.
- Potential signs of data being exfiltrated from the network, which may include:
    - Abnormal amount of data outgoing over any port. Open source software can tunnel data over various ports and protocols. For example, ransomware actors have used Chisel to tunnel Secure Shell (SSH) over HTTPS port `443`. Ransomware actors have also used Cloudflared to abuse Cloudflare tunnels to tunnel communications over HTTPS.
    - Presence of Rclone, Rsync, and various web-based file storage services, and FTP/SFTP, which are common tools for data exfiltration (and also used by threat actors to implant malware/tools on affected networks.)
- Newly created services, unexpected scheduled tasks, unexpected software installed, unusual files created, legitimate processes with unexpected child processes, etc.

□ For cloud environments:

- Enable tools to detect and prevent modifications to IAM, network security, and data protection resources.
- Use automation to detect common issues (e.g., disabling features, introduction of new firewall rules) and take automated actions as soon as they occur. For example, if a new firewall rule is created that allows open traffic (`0.0.0.0/0`), an automated action can be taken to disable or delete this rule and send notifications to the user that created it as well as the security team for awareness. This will help avoid alert fatigue and allow security personnel to focus on critical issues.

Reporting and Notification

Note: Refer to the Contact Information section at the end of this guide for details on how to report and notify about ransomware incidents.

- ☐ **7.** Follow notification requirements as outlined in your cyber incident response and communications plan to **engage internal and external teams and stakeholders** with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.
  - ☐ Share the information you have at your disposal to receive timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders [CPG 4.A].
  - ☐ Report the incident to—and consider requesting assistance from—CISA, your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or your local U.S. Secret Service field office.
  - ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.

If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- Recovered executable file.
- Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible.
- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally).
- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally).
- Malware samples.
- Names of malware identified on your network.
- Encrypted file samples.
- Log files (e.g., Windows event logs from compromised systems, firewall logs).
- PowerShell scripts found having executed on the network.
- User accounts created in AD or machines added to the network during the exploitation.
- Email addresses used by the attackers and any associated phishing emails.
- Other communication accounts used by the attackers.
- A copy of the ransom note.
- Ransom amount and if the ransom was paid.
- Bitcoin wallets used by the attackers.
- Bitcoin wallets used to pay the ransom, if applicable.
- Copies of any communications with attackers.

- ☐ **8.** If the incident resulted in a data breach, **follow notification requirements as outlined in your cyber incident response and communications plans.**

Containment and Eradication

If no initial mitigation actions appear possible:

- ☐ **9. Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers).** Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.
  - ☐ Preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

Upon voluntary request, CISA and MS-ISAC (for SLTT organizations) can assist with analysis of phishing emails, storage media, logs, and/or malware at no cost to help organizations understand the root cause of an incident.

- CISA – Advanced Malware Analysis Center: malware.us-cert.gov/
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/

- ☐ **10. Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available,** as security researchers may have discovered encryption flaws for some ransomware variants and released decryption or other types of tools.

To continue taking steps to contain and mitigate the incident:

- ☐ **11. Research trusted guidance** (e.g., published by sources such as the U.S. Government, MS-ISAC, or a reputable security vendor) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.
  - ☐ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known associated registry values and files.

- ☐ **12. Identify the systems and accounts involved in the initial breach.** This can include email accounts.

- ☐ **13.** Based on the breach or compromise details determined above, **contain associated systems that may be used for further or continued unauthorized access.** Breaches often involve mass credential exfiltration. Securing networks and other information sources from continued credential-based unauthorized access may include:
  - ☐ Disable virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ **14.** If server-side data is being encrypted by an infected workstation, **follow server-side data encryption quick identification steps.**

- ☐ Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.
- ☐ Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.
- ☐ Review the `TerminalServices-RemoteConnectionManager` event log to check for successful RDP network connections.
- ☐ Review the Windows Security log, SMB event logs, and related logs that may identify significant authentication or access events.
- ☐ Run packet capture software, such as Wireshark, on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., `smb2.filename contains cryptxxx`).

☐ **15. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.**

- ☐ Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
- ☐ Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
- ☐ Identification may involve deployment of EDR solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

☐ **16. Rebuild systems based on prioritization of critical services** (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible. Use infrastructure as code templates to rebuild cloud resources.

☐ **17. Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility** once the environment has been fully cleaned and rebuilt, including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms. This can include applying patches, upgrading software, and taking other security precautions not previously taken. Update customer-managed encryption keys as needed.

☐ **18. The designated IT or IT security authority declares the ransomware incident over** based on established criteria, which may include taking the steps above or seeking outside assistance**.**

Recovery and Post-Incident Activity

- ☐ **19. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.**
  - ☐ Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network (VLAN) has been created for recovery purposes, ensure only clean systems are added.

- ☐ **20. Document lessons learned from the incident and associated response activities** to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.

- ☐ **21. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC** to benefit others within the community.

Contact Information

In responding to any cyber incident, federal agencies will undertake threat response; asset response; and intelligence support and related activities.

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents.
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant).
- Phishing email, storage media, log, and malware analysis based on voluntary submission. Full-disk forensics can be performed on an as-needed basis.
- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, including system images and malware samples.

Federal Asset Response Contacts

Upon voluntary request, federal asset response includes furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.

CISA:	cisa.gov/report Central@cisa.gov or call (888) 282-0870 Cybersecurity Advisor (cisa.gov/cisa-regions): [Enter your local CISA CSA's phone number and email address.]
MS-ISAC:	For SLTTs, email soc@msisac.org or call (866) 787-4722

Federal Threat Response Contacts

Upon voluntary request, or upon notification of partners, federal threat response includes conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

FBI:	fbi.gov/contact-us/field-offices [Enter your local FBI field office POC phone number and email address.]
USSS:	FBI Internet Crime Complaint Center (IC3) at ic3.gov secretservice.gov/contact/field-offices/ [Enter your USSS field office POC phone number and email address.]

Other Federal Response Contacts

NSA: Cybersecurity Collaboration Center Services and Contact Information

Other Response Contacts

Consider filling out Table 1 for use should your organization become affected by ransomware. Consider contacting these organizations for mitigation and response assistance or for notification.

Table 1: Response Contacts Information

Response Contacts:		
Contact	**24x7 Contact Information**	**Roles and Responsibilities**
IT/IT Security Team – Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

RESOURCES

CISA No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) is bi-directional. This includes best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware.
- Policy-oriented or technical assessments help organizations understand how they can improve their defenses to avoid ransomware infection: cisa.gov/cyber-resource-hub.
    - o Assessments include no-cost vulnerability scanning.
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario: cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.
- CISA cybersecurity advisors advise on best practices and connect you with CISA resources to manage cyber risk.
- Cyber Security Evaluation Tool (CSET) guides asset owners and operators through a systematic process of evaluating operational technology (OT) and IT. CSET includes the Ransomware Readiness Assessment (RRA), a self-assessment based on a tiered set of practices to help organizations evaluate how well they are equipped to defend and recover from a ransomware incident.

Contacts:

- SLTT and private sector organizations: CISA.JCDC@cisa.dhs.gov

Ransomware Quick References

- StopRansomware.gov—a whole-of-government website that gives ransomware resources and alerts.
- Security Primer – Ransomware (MS-ISAC)—outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations.
- Institute for Security + Technology (IST) Blueprint for Ransomware Defense—an action plan for ransomware mitigation, response, and recovery for small- and medium-sized enterprises.

Additional Resources

- NIST: Zero Trust Architecture
- CISA: Cloud Security Technical Reference Architecture
- CISA: Secure Cloud Business Applications (SCuBA) Project
- CISA: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses
- CISA: Protecting Against Cyber Threats to Managed Service Providers and their Customers
- NSA: Mitigating Cloud Vulnerabilities (NSA)

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

PURPOSE

This document was developed in furtherance of the authors' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

ACKNOWLEDGEMENTS

Microsoft contributed to this joint guide.

SUBSCRIBE SIGN IN

HOW MANY TEACHERS DOES IT TAKE TO DEBUG A SMART LIGHTING SYSTEM? —

US school runs lights 24/7/365: The smart lights have been broken since 2021

"We've been doing everything we can to fix this," says school official.

RON AMADEO - 1/20/2023, 6:20 PM

Minnechaug Regional High School

Enlarge / The Minnechaug Regional High School.

The lights at Massachusetts' Minnechaug Regional High School burn ever bright. They actually never turn off. They *can't* turn off. The smart lighting system for the entire building is broken, and it's stuck in the "on" position. It has apparently been this way for *over a year now*, and the electric bills are really starting to pile up.

“We are very much aware this is costing taxpayers a significant amount of money,” the school district's assistant superintendent of finance, Aaron Osborne, told NBC News. “And we have been doing everything we can to get this problem solved.”

The school's entire "green lighting system," some 7,000 lights, was installed over a decade ago and was *supposed* to save money, but according to the report, "the software that runs it failed on Aug. 24, 2021" and no one has been able to turn off the lights for the following 17 months. Teachers are adjusting by unscrewing light bulbs at the end of the day and throwing some breakers not connected to vital parts of the school. Dimming the lights to show movies or something projected on a whiteboard has also been difficult: The lights are on full brightness all the time.

News Editor Lilli DiGrande, writing for Minnechaug student newspaper The Smoke Signal, did some great reporting on the situation a month after it started. The smart lighting company that installed the lights over 10 years ago, 5th Light, has apparently changed hands several times now and is currently owned by a company called Reflex Lighting. According to the Smoke Signal report, what's left of 5th Light no longer has access to the old proprietary software to fix anything, so "fixing" the system means replacing it with new hardware.

FURTHER READING
Insteon finally comes clean about its sudden smart home shutdown

The problem with new parts is that this has all been in the middle of the pandemic and a huge chip shortage, so the parts have been back-ordered and delayed several times. The process of fixing the system was originally supposed to start in February 2022, but they can't get the parts. The next missed date was October 2022, and the school isn't expecting a repair until February 2023. The lights remain on.

A lesson in proper smart building design

Even if you aren't in charge of the lighting design of a giant building, there's a valuable lesson here for anyone getting involved with smart home/building technology: make technology an *addition* to your setup, not a *dependency*. You still need to install physical light switches in every room, but as a bonus, you can pick light switches that are also controllable via some kind of network. All sorts of smart light switches meet this requirement—normal paddles or even toggles that can also be controlled via Zigbee, Z-Wave, Bluetooth, Wi-Fi, probably Ethernet, or whatever you want. This way, if the Internet is down, or some server explodes, or some cloud company shuts down, the lights will still work.

What you definitely *shouldn't* do is hard-wire the electricity to be always on and then hope the network to the light fixtures or light bulbs will be around to power them off. That's apparently what happened at this school, and now taxpayers are paying the price.

READER COMMENTS 340

RON AMADEO
Ron is the Reviews Editor at Ars Technica, where he specializes in Android OS and Google products. He is always on the hunt for a new gadget and loves to rip things apart to see how they work. He loves to tinker and always seems to be working on a new project.

Contact Us

BLOG QUICKTIPS

What to know in the wake of cyberattack on children's hospital.

Children's hospital cyberattack: vulnerabilities & solutions in healthcare security.

Last week, Lurie Children's Hospital in Chicago revealed details about a recent cyberattack that left them without access to phone lines, email accounts, and other online communications.

After confirming that the cyberattack was instigated "by a known criminal threat actor," hospital officials said they were working with the FBI to determine how the hack happened and get the institution back to normal operations.

Contact Us

functioning like normal. But as the hospital enters the third week of disruptions, the incident underscores the vulnerability of healthcare organizations to cyberthreats.

As of the time of writing, phone calls to Lurie Children’s Hospital are being re-routed to an external call center. Patients cannot access electronic medical records or lab results. Providers are struggling to schedule appointments and make critical care decisions. And no one knows whether protected health information has been leaked on the dark web.

How was Lurie Children’s Hospital attacked?

So far, the specifics of the attack are unknown. But cybersecurity experts assume it came via a ransomware attempt. Defined as a type of malicious software designed to encrypt files and demand payment in exchange for their release, ransomware has devastated many North American healthcare organizations in recent years. In fact, the FBI received more reports of ransomware attacks on the healthcare sector in 2022 than any other critical infrastructure industry. Moreover, in 2023, ransomware payments hit a record $1.1 billion, highlighting the increasing rate and financial impact of these attacks.

Why are hackers targeting healthcare organizations?

Because they have come to view such institutions as easy targets. Hospitals manage hundreds of thousands of sensitive patient records and are more likely to fork over ransom payments to shield them while trying to keep essential services running.

Since so many high–profile hacks have targeted the healthcare industry in recent years, cybersecurity professionals believe the industry faces a critical juncture in its ongoing battle. Lurie Children’s Hospital has assured patients and their families that they are prioritizing the confidentiality and integrity of medical information. But many worry that it’s already too late to prevent unauthorized access or disclosure.

What can healthcare organizations do to protect themselves?

In light of this cyberattack, IT providers like CMIT Solutions are urging businesses in the healthcare industry to reevaluate their cybersecurity measures and bolster their defenses. This includes

Contact Us

Implement multi-layered cybersecurity measures. These range from broad-based security for all systems to specific protections for electronic medical records and medical scheduling. At CMIT Solutions, we recommend a diverse approach that includes advanced firewalls, intrusion detection systems, and endpoint encryption for every device. It's also critical to regularly update and patch software and systems and to mitigate the risk of exploitation.

Conduct regular security audits, risk assessments, and incident response reviews. Working with a trusted IT partner, companies operating in every sector should undertake comprehensive cybersecurity audits to identify potential vulnerabilities and weaknesses in your organization's infrastructure. Risk assessments can outline the potential impact of cyberthreats, while simulated incident response protocols can help employees know what actions to take to protect information in the event of a problem.

Provide ongoing employee education and training. If the Lurie Children's Hospital attack is traced back to ransomware, cybersecurity experts will likely point to human error as the cause of the infection. When employees know how to spot phishing attempts, strengthen passwords, and follow cybersecurity protocols, the chances of negative impacts decrease. Healthcare businesses should also implement clear policies and procedures for the secure handling of sensitive data.

Back up critical information regularly. Many cybersecurity experts speculate that Lurie Children's Hospital either did not have sufficient data backups in place—or housed them on devices connected to their main network, allowing them to be infected when the ransomware struck. If data is backed up regularly, remotely, and redundantly (i.e., stored in multiple on-site and off-site locations), businesses can quickly bounce back from ransomware attacks by wiping affected systems clean and rebooting from a recent backup.

Establish incident response plans. It's also important to have procedures and protocols in place in the event of an attack. These response plans involve testing backup systems to verify

Contact Us

Maintain regulatory compliance. Any business operating in the healthcare industry is required to comply with relevant regulations and standards like HIPAA (the Health Insurance Portability and Accountability Act). More importantly, any HIPAA violation can lead to civil and criminal penalties, substantial monetary fines, and reputational impacts that are difficult to recover from.

Work with a trusted expert in your community. Not sure how to wrap your head around the long list of recommendations outlined above? Established IT service providers like CMIT Solutions can help to understand emerging threats, promote threat intelligence, implement cybersecurity best practices, and respond when incidents occur. Most importantly, a fellow business owner rooted in your local community will understand the need to solve short-term problems while positioning your company to make sound financial investments that lead to long-term success.

The recent cyberattack on Lurie Children's Hospital serves as a stark reminder of the dangers facing healthcare organizations. And fear and uncertainty about the digital landscape can leave many businesses vulnerable to digital risk.

At CMIT Solutions, we work hard to protect data, secure networks, and empower employees. As a large North American system with more than 25 years of experience and 250-plus offices across the United States and Canada, we deliver threat protection and trusted advice to every client.

Whether you're a large healthcare system looking for operational stability or a small office that needs to upgrade its computer systems, CMIT Solutions can help. Contact us today to prevent ransomware and ensure a safer future for your business.

Back to Blog

Share:

Contact Us

Request Consultation

Contact Us

LOCATIONS

FRANCHISE OPPORTUNITIES

SUBSCRIBE TO QUICKTIPS

Enter Your Email

Subscribe

ALSO OF INTEREST

IT Support and Maintenance to Cybersecurity

IT Managed Services for Secured Technology

Cloud Security for Business-Specific Experience

Privacy Policy Accessibility

PREPARE FOR A CYBER BREACH AT YOUR CONFERENCE TABLE

By Thomas DeMayo, Partner and Robert Gaines, Director

The statement “It is not a matter of if, but when, a cyber breach will occur” has held true as cyber incidents continue to escalate in severity and sophistication. While a major cybersecurity incident will always be stressful, ensuring stakeholders understand their roles and have defined responses should shift from what would inherently be a chaotic and unorchestrated sequence of events into a controlled and managed response.

Tabletop Exercises

A tabletop exercise takes the pieces of paper on which your incident response plan is inked and turns it into a simulated exercise where the players rehearse their roles. Like a well-crafted play, everyone has a part that – when joined together – tells a story. If well written, it can be a story of success and triumph.

Tabletop exercises use real-world threat scenarios to simulate a security incident and provide an opportunity to identify potential risks and vulnerabilities within an organization’s processes, systems and personnel that drive the overall response. For example, the exercise may simulate a Ransomware event that locks down systems requiring the activation of the Business Continuity Plan **and** the exfiltration of data, requiring breach reporting obligations to regulatory parties and individuals. This approach ensures that an organization’s incident response plans are up-to-date and effective, and they provide management with an excellent tool to evaluate the organization’s response readiness.

Evaluation outcomes are used to adjust items such as end-user training, supplementary training for first responders, modification of security controls or implementation of new security tools.

Incident Players

For a tabletop exercise to be effective, it needs to involve multiple stakeholders. The leader and orchestrator of the tabletop exercise needs to design the scenarios to facilitate communication and coordination among different teams and departments from incident identification to an incident.

Because incident communication is performed at different levels within the organization, testing should also be performed and evaluated at different operational levels:

- *Board/Executive* – The Board and senior management play an essential role in any major incident. They are the commanders making key decisions that will have outcomes that will impact not only the business' bottom line but also the underlying reputation and trust of the business. Participants are Board members, C-Suite executives and the CISO, CIO or CTO.

- *Managerial* – The management level drives the operational response to incidents through decision-making and coordination with responsible departments, vendors and third parties. Participants generally include management from IT, Security, Risk and Operations departments, as well as key vendors where possible.

- *Operational* – The front-line responders facilitate the procedural incident response activity coordination, triage, escalation communications and alignment with the incident response plan procedures. Participants typically include first responders, security and technology subject matter experts and their managers.

Best Practice: Cyber Response Testing

Many industries and regulatory bodies such as the Health Insurance Portability and Accountability Act (HIPAA), Federal Financial Institutions Examination Council (FFIEC), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) and New York State Department of Financial Services (NYDFS) require organizations to have incident response plans in place and that they be tested regularly. In addition, many insurance companies require proof of testing before they provide coverage for cybersecurity incidents, with many policies stipulating annual testing as a component of insurance renewal. Annual testing is a recommended best practice, as the tabletop exercises should be an element of any institution's annual security and risk assessment review process.

Many organizations have also invested in either in-house security operation teams or a third-party SOC-as-a-Service to drive the technical components of the plan. While different from a table-top exercise, exercises can be developed to test the tools and responses of these teams. Such exercises help validate that the Security Operations Team's tools and processes are correctly tuned to detect attacks and ensure a timely response.

At PKF O'Connor Davies, we have a team of cybersecurity and business continuity specialists who can help you design and conduct a tabletop exercise or test the security tools and teams in which you have invested. If you have any questions, please contact your client service team or either of the following:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Robert Gaines, CISSP, CECI, CCFI, CIPP/US
Director
Cybersecurity and Privacy Advisory
rgaines@pkfod.com | 425.518.1974

MEDIA CONTACT

Posted In: Articles
Posted On: March 8, 2024

Older Entry »

Menu

SHARE:

ALERT

FBI, CISA, and ASD's ACSC Release Advisory on Play Ransomware

Release Date: December 18, 2023

RELATED TOPICS: CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>, MALWARE, PHISHING, AND RANSOMWARE </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

Today, the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Play Ransomware <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>, to disseminate Play ransomware group's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as October 2023.

Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data and have impacted a wide range of businesses and critical infrastructure organizations in North America, South America, Europe, and Australia.

FBI, CISA, and the ASD's ACSC encourage organizations review and implement the recommendations provided in the joint CSA to reduce the likelihood and impact of Play and other ransomware incidents. For more information, see CISA's #StopRansomware <https://www.cisa.gov/stopransomware> webpage, which includes the updated #StopRansomware Guide <https://www.cisa.gov/stopransomware/ransomware-guide>.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

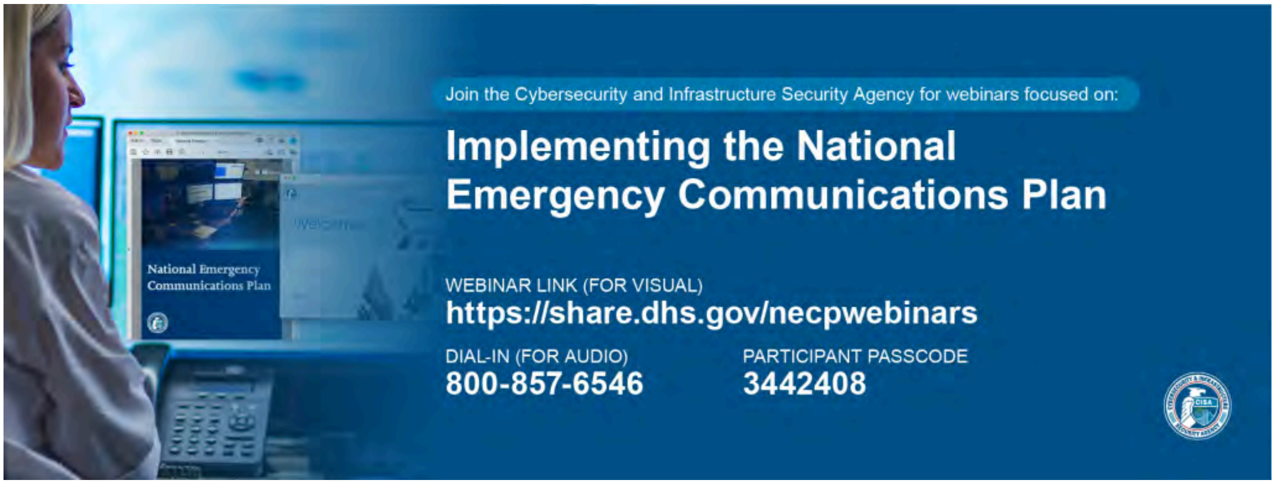
Topics: Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Malware, Phishing, and Ransomware </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

Menu

SHARE:

NECP Webinars

<https://share.dhs.gov/necpwebinars>



Join the Cybersecurity and Infrastructure Security Agency for webinars focused on:

Implementing the National Emergency Communications Plan

WEBINAR LINK (FOR VISUAL)
https://share.dhs.gov/necpwebinars

DIAL-IN (FOR AUDIO)
800-857-6546

PARTICIPANT PASSCODE
3442408

The National Emergency Communications Plan (NECP) webinar series is designed to provide the public safety community with practical solutions intended to help organizations improve their emergency communications capabilities through the implementation of the NECP.

2023 Webinars

APR 26, 2023 **OTHER | VIRTUAL/ONLINE**

Is This Thing On? Using Backup Communications Systems To Ensure Mission Readiness </news-events/events/thing-using-backup-communications-systems-ensure-mission-readiness>

JUN 07, 2023 **VIRTUAL/ONLINE**

Using Data to Drive Decisions: The SAFECOM Nationwide Survey </news-events/events/using-data-drive-decisions-safecom-nationwide-survey>

</news-events/events/ready-resilient-cyber-incident-response-strategies-emergency-communications>

OCT 25, 2023 **SEMINAR | VIRTUAL/ONLINE**

Ready & Resilient: Cyber Incident Response Strategies for Emergency Communications

</news-events/events/ready-resilient-cyber-incident-response-strategies-emergency-communications>

Archived 2022 Webinars

OCT 10, 2022 **TRAINING | VIRTUAL/ONLINE**

Be Prepared! Cyber Incident Response Planning for Emergency Communications </news-events/events/be-prepared-cyber-incident-response-planning-emergency-communications>

JUN 15, 2022 **TRAINING | VIRTUAL/ONLINE**

How is 5G Impacting Emergency Communications? </news-events/events/how-5g-impacting-emergency-communications>

MAR 09, 2022 **TRAINING | VIRTUAL/ONLINE**

Money Talks: Funding Your Emergency Communications Capabilities </news-events/events/money-talks-funding-your-emergency-communications-capabilities>

Archived 2021 Webinars

DEC 15, 2021 **TRAINING | VIRTUAL/ONLINE**

Stay Flexible and Adaptable: Planning for Communications Continuity </news-events/events/stay-flexible-and-adaptable-planning-communications-continuity>

OCT 15, 2021 **TRAINING | VIRTUAL/ONLINE**

Addressing the Ransomware Threat to Emergency Communications </news-events/events/addressing-ransomware-threat-emergency-communications>

SEP 15, 2021 **TRAINING | VIRTUAL/ONLINE**

Planning for Emerging Communications Technology </news-events/events/planning-emerging-communications-technology>

MAY 26, 2021 **TRAINING | VIRTUAL/ONLINE**

It Takes a Village: Leveraging the Whole Community to Make Critical Emergency Communications Decisions </news-events/events/it-takes-village-leveraging-whole-community-make-critical-emergency-communications-decisions>

APR 14, 2021 **TRAINING | VIRTUAL/ONLINE**

Jump to the Head of the Line! Priority Services for Emergency Communications </news-events/events/jump-head-line-priority-services-emergency-communications>

MAR 17, 2021 **TRAINING | VIRTUAL/ONLINE**

Train and Exercise to Help Public Safety Personnel Overcome Information Overload, Stress, and Trauma </news-events/events/train-and-exercise-help-public-safety-personnel-overcome-information-overload-stress-and-trauma>

Archived 2020 Webinars

JUL 15, 2021 **TRAINING | VIRTUAL/ONLINE**

How Does Your Agency Start to Improve Its Cybersecurity Posture? Implement the NIST Cybersecurity Framework. </news-events/events/how-does-your-agency-start-improve-its-cybersecurity-posture-implement-nist-cybersecurity-framework>

AUG 19, 2020 **TRAINING | VIRTUAL/ONLINE**

Make the Most of Your Organization’s Investments: Lifecycle Planning for Emergency Communications </news-events/events/make-most-your-organizations-investments-lifecycle-planning-emergency-communications>

SEP 17, 2020 **TRAINING | VIRTUAL/ONLINE**

EXERCISE! EXERCISE! EXERCISE! Learn How to Turn Evaluations Into Real-World Communications Improvements. </news-events/events/exercise-exercise-exercise-learn-how-turn-evaluations-real-world-communications-improvements>

MAR 09, 2022 **TRAINING | VIRTUAL/ONLINE**

Money Talks: Funding Your Emergency Communications Capabilities </news-events/events/money-talks-funding-your-emergency-communications-capabilities>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

888-282-0870 central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility </accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

SHARE:

CYBERSECURITY ADVISORY

Scattered Spider

Release Date: November 16, 2023 **Alert Code:** AA23-320A

RELATED TOPICS: CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>, MALWARE, PHISHING, AND RANSOMWARE </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) in response to recent activity by Scattered Spider threat actors against the commercial facilities sectors and subsectors. This advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations as recently as November 2023.

Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs.

The FBI and CISA encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of a cyberattack by Scattered Spider actors.

Download the PDF version of this report:

AA23-320A Scattered Spider </sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf> (PDF, 510.78 KB)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v14/matrices/enterprise/> framework, version 14. See the MITRE ATT&CK® Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping> and CISA's Decider Tool <https://github.com/cisagov/decider/>.

Overview

Scattered Spider (also known as Starfraud, UNC3944, Scatter Swine, and Muddled Libra) engages in data extortion and several other criminal activities.[1 <https://attack.mitre.org/versions/v14/groups/g1015/>] Scattered Spider threat actors are considered experts in social engineering and use multiple social engineering techniques, especially phishing, push bombing, and subscriber identity module (SIM) swap attacks, to obtain credentials, install remote access tools, and/or bypass multi-factor authentication (MFA). According to public reporting, Scattered Spider threat actors have [2 <https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html>],[3 <https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/>],[4 <https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/>]:

- Posed as company IT and/or helpdesk staff using phone calls or SMS messages to obtain credentials from employees and gain access to the network [T1598 <https://attack.mitre.org/versions/v14/techniques/t1598/>],[T1656 <https://attack.mitre.org/versions/v14/techniques/t1656/>].
- Posed as company IT and/or helpdesk staff to direct employees to run commercial remote access tools enabling initial access [T1204 <https://attack.mitre.org/versions/v14/techniques/t1204/>],[T1219 <https://attack.mitre.org/versions/v14/techniques/t1219/>],[T1566 <https://attack.mitre.org/versions/v14/techniques/t1566/>].

- Posed as IT staff to convince employees to share their one-time password (OTP), an MFA authentication code.
- Sent repeated MFA notification prompts leading to employees pressing the "Accept" button (also known as MFA fatigue) [T1621 <https://attack.mitre.org/versions/v14/techniques/t1621/>].[5 <https://www.malwarebytes.com/blog/personal/2023/09/ransomware-group-steps-up-issues-statement-over-mgm-resorts-compromise>]
- Convinced cellular carriers to transfer control of a targeted user's phone number to a SIM card they controlled, gaining control over the phone and access to MFA prompts.
- Monetized access to victim networks in numerous ways including extortion enabled by ransomware and data theft [T1657 <https://attack.mitre.org/versions/v14/techniques/t1657/>].

After gaining access to networks, the FBI observed Scattered Spider threat actors using publicly available, legitimate remote access tunneling tools. Table 1 details a list of legitimate tools Scattered Spider, repurposed and used for their criminal activity. **Note:** The use of these legitimate tools alone is not indicative of criminal activity. Users should review the Scattered Spider indicators of compromise (IOCs) and TTPs discussed in this CSA to determine whether they have been compromised.

Table 1: Legitimate Tools Used by Scattered Spider

Tool	Intended Use
Fleetdeck.io	Enables remote monitoring and management of systems.
Level.io	Enables remote monitoring and management of systems.
Mimikatz [S0002 <https://attack.mitre.org/versions/v14/software/s0002/>]	Extracts credentials from a system.

Tool	Intended Use
Ngrok [S0508 <https://attack.mitre.org/versions/v14/software/s0508/>]	Enables remote access to a local web server by tunneling over the internet.
Pulseway	Enables remote monitoring and management of systems.
Screenconnect	Enables remote connections to network devices for management.
Splashtop	Enables remote connections to network devices for management.
Tactical.RMM	Enables remote monitoring and management of systems.
Tailscale	Provides virtual private networks (VPNs) to secure network communications.
Teamviewer	Enables remote connections to network devices for management.

In addition to using legitimate tools, Scattered Spider also uses malware as part of its TTPs. See Table 2 for some of the malware used by Scattered Spider.

Table 2: Malware Used by Scattered Spider

Malware	Use
AveMaria (also known as WarZone [S0670 <https://attack.mitre.org/versions/v14/software/s0670/>])	Enables remote access to a victim's systems.

Malware	Use
Raccoon Stealer	Steals information including login credentials [TA0006 <https://attack.mitre.org/versions/v14/tactics/ta0006/>], browser history [T1217 <https://attack.mitre.org/versions/v14/techniques/t1217/>], cookies [T1539 <https://attack.mitre.org/versions/v14/techniques/t1539/>], and other data.
VIDAR Stealer	Steals information including login credentials, browser history, cookies, and other data.

Scattered Spider threat actors have historically evaded detection on target networks by using living off the land techniques and allowlisted applications to navigate victim networks, as well as frequently modifying their TTPs.

Observably, Scattered Spider threat actors have exfiltrated data [TA0010 <https://attack.mitre.org/versions/v14/tactics/ta0010/>] after gaining access and threatened to release it without deploying ransomware; this includes exfiltration to multiple sites including U.S.-based data centers and MEGA[.]NZ [T1567.002 <https://attack.mitre.org/versions/v14/techniques/t1567/002/>].

Recent Scattered Spider TTPs

New TTP - File Encryption

More recently, the FBI has identified Scattered Spider threat actors now encrypting victim files after exfiltration [T1486 <https://attack.mitre.org/versions/v14/techniques/t1486/>]. After exfiltrating and/or encrypting data, Scattered Spider threat actors communicate with victims via TOR, Tox, email, or encrypted applications.

Reconnaissance, Resource Development, and Initial Access

Scattered Spider intrusions often begin with broad phishing [T1566 <https://attack.mitre.org/versions/v14/techniques/t1566/>] and smishing [T1660 <https://attack.mitre.org/versions/v14/techniques/t1660/>] attempts against a target using victim-specific crafted domains, such as the domains listed in Table 3 [T1583.001 <https://attack.mitre.org/versions/v14/techniques/t1583/001/>].

Table 3: Domains Used by Scattered Spider Threat Actors

Domains
victimname-sso[.]com
victimname-servicedesk[.]com
victimname-okta[.]com

In most instances, Scattered Spider threat actors conduct SIM swapping attacks against users that respond to the phishing/smishing attempt. The threat actors then work to identify the personally identifiable information (PII) of the most valuable users that succumbed to the phishing/smishing, obtaining answers for those users' security questions. After identifying usernames, passwords, PII [T1589 <https://attack.mitre.org/versions/v14/techniques/t1589/>], and conducting SIM swaps, the threat actors then use social engineering techniques [T1656 <https://attack.mitre.org/versions/v14/techniques/t1656/>] to convince IT help desk personnel to reset passwords and/or MFA tokens [T1078.002 <https://attack.mitre.org/versions/v14/techniques/t1078/002/>], [T1199 <https://attack.mitre.org/versions/v14/techniques/t1199/>],[T1566.004 <https://attack.mitre.org/versions/v14/techniques/t1566/004/>] to perform account takeovers against the users in single sign-on (SSO) environments.

Execution, Persistence, and Privilege Escalation

Scattered Spider threat actors then register their own MFA tokens [T1556.006 <https://attack.mitre.org/versions/v14/techniques/t1556/006/>],[T1606 <https://attack.mitre.org/versions/v14/techniques/t1606/>] after compromising a user's account to establish persistence [TA0003 <https://attack.mitre.org/versions/v14/tactics/ta0003/>]. Further, the threat actors add a federated identity provider to the victim's SSO tenant and activate automatic account linking [T1484.002 <https://attack.mitre.org/versions/v14/techniques/t1484/002/>]. The threat actors are then able to sign into any account by using a matching SSO account attribute. At this stage, the Scattered Spider threat actors already control the identity provider and then can choose an arbitrary value for this account attribute. As a result, this activity allows the threat actors to perform privileged escalation [TA0004 <https://attack.mitre.org/versions/v14/tactics/ta0004/>] and continue logging in even when passwords are changed [T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>]. Additionally, they leverage common endpoint detection and response (EDR) tools installed on the victim networks to take advantage of the tools' remote-shell capabilities and executing of commands which elevates their access. They also deploy remote monitoring and management (RMM) tools [T1219 <https://attack.mitre.org/versions/v14/techniques/t1219/>] to then maintain persistence.

Discovery, Lateral Movement, and Exfiltration

Once persistence is established on a target network, Scattered Spider threat actors often perform discovery, specifically searching for SharePoint sites [T1213.002 <https://attack.mitre.org/versions/v14/techniques/t1213/002/>], credential storage documentation [T1552.001 <https://attack.mitre.org/versions/v14/techniques/t1552/001/>], VMware vCenter infrastructure [T1018 <https://attack.mitre.org/versions/v14/techniques/t1018/>], backups, and instructions for setting up/logging into Virtual Private Networks (VPN) [TA0007 <https://attack.mitre.org/versions/v14/tactics/ta0007/>]. The threat actors enumerate the victim's Active Directory (AD), perform discovery and exfiltration of victim's code repositories [T1213.003 <https://attack.mitre.org/versions/v14/techniques/t1213/003/>], code-signing certificates [T1552.004 <https://attack.mitre.org/versions/v14/techniques/t1552/004/>], and source code [T1083 <https://attack.mitre.org/versions/v14/techniques/t1083/>],[TA0010 <https://attack.mitre.org/versions/v14/tactics/ta0010/>]. Threat actors activate Amazon Web Services (AWS) Systems Manager Inventory [T1538 <https://attack.mitre.org/versions/v14/techniques/t1538/>] to discover targets for lateral movement [TA0007 <https://attack.mitre.org/versions/v14/tactics/ta0007/>],[TA0008 <https://attack.mitre.org/versions/v14/tactics/ta0008/>], then move to both preexisting [T1021.007 <https://attack.mitre.org/versions/v14/techniques/t1021/007/>] and actor-created [T1578.002 <https://attack.mitre.org/versions/v14/techniques/t1578/002/>] Amazon Elastic Compute Cloud (EC2) instances. In instances where the ultimate goal is data exfiltration, Scattered Spider threat actors use actor-installed extract, transform, and load (ETL) tools [T1648 <https://attack.mitre.org/versions/v14/techniques/t1648/>] to bring data from multiple data sources into a centralized database [T1074 <https://attack.mitre.org/versions/v14/techniques/t1074/>],[T1530 <https://attack.mitre.org/versions/v14/techniques/t1530/>]. According to trusted third parties, where more recent incidents are concerned, Scattered Spider threat actors may have deployed BlackCat/ALPHV ransomware onto victim networks—thereby encrypting VMware Elastic Sky X integrated (ESXi) servers [T1486 <https://attack.mitre.org/versions/v14/techniques/t1486/>].

To determine if their activities have been uncovered and maintain persistence, Scattered Spider threat actors often search the victim's Slack, Microsoft Teams, and Microsoft Exchange online for emails [T1114 <https://attack.mitre.org/versions/v14/techniques/t1114/>] or conversations regarding the threat actor's intrusion and any security response. The threat actors frequently join incident remediation and response calls and teleconferences, likely to identify how security teams are hunting them and proactively develop new avenues of intrusion in response to victim defenses. This is sometimes achieved by creating new identities in the environment [T1136 <https://attack.mitre.org/versions/v14/techniques/t1136/>] and is often upheld with fake social media profiles [T1585.001 <https://attack.mitre.org/versions/v14/techniques/t1585/001/>] to backstop newly created identities.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 4 through 17 for all referenced threat actor tactics and techniques in this advisory.

Table 4: Reconnaissance

Technique Title	**ID**	**Use**
Gather Victim Identity Information	T1589 <https://attack.mitre.org/versions/v14/techniques/t1589/>	Scattered Spider threat actors gather usernames, passwords, and PII for targeted organizations.
Phishing for Information	T1598 <https://attack.mitre.org/versions/v14/techniques/t1598/>	Scattered Spider threat actors use phishing to obtain login credentials, gaining access to a victim's network.

Table 5: Resource Development

Technique Title	**ID**	**Use**

Technique Title	ID	Use
Acquire Infrastructure: Domains	T1583.001 <https://attack.mitre.org/versions/v14/techniques/t1583/001/>	Scattered Spider threat actors create domains for use in phishing and smishing attempts against targeted organizations.
Establish Accounts: Social Media Accounts	T1585.001 <https://attack.mitre.org/versions/v14/techniques/t1585/001/>	Scattered Spider threat actors create fake social media profiles to backstop newly created user accounts in a targeted organization.

Table 6: Initial Access

Technique Title	ID	Use
Phishing	T1566 <https://attack.mitre.org/versions/v14/techniques/t1566/>	Scattered Spider threat actors use broad phishing attempts against a target to obtain information used to gain initial access. Scattered Spider threat actors have posed as helpdesk personnel to direct employees to install commercial remote access tools.

Technique Title	ID	Use
Phishing (Mobile)	T1660 <https://attack.mitre.org/versions/v14/techniques/t1660/>	Scattered Spider threat actors send SMS messages, known as smishing, when targeting a victim.
Phishing: Spearphishing Voice	T1566.004 <https://attack.mitre.org/versions/v14/techniques/t1566/004/>	Scattered Spider threat actors use voice communications to convince IT help desk personnel to reset passwords and/or MFA tokens.
Trusted Relationship	T1199 <https://attack.mitre.org/versions/v14/techniques/t1199/>	Scattered Spider threat actors abuse trusted relationships of contracted IT help desks to gain access to targeted organizations.
Valid Accounts: Domain Accounts	T1078.002 <https://attack.mitre.org/versions/v14/techniques/t1078/002/>	Scattered Spider threat actors obtain access to valid domain accounts to gain initial access to a targeted organization.

Table 7: Execution

Technique Title	ID	Use

Technique Title	ID	Use
Serverless Execution	T1648 <https://attack.mitre.org/versions/v14/techniques/t1648/>	Scattered Spider threat actors use ETL tools to collect data in cloud environments.
User Execution	T1204 <https://attack.mitre.org/versions/v14/techniques/t1204/>	Scattered Spider threat actors impersonating helpdesk personnel direct employees to run commercial remote access tools thereby enabling access to the victim's network.

Table 8: Persistence

Technique Title	ID	Use
Persistence	TA0003 <https://attack.mitre.org/versions/v14/tactics/ta0003/>	Scattered Spider threat actors seek to maintain persistence on a targeted organization's network.
Create Account	T1136 <https://attack.mitre.org/versions/v14/techniques/t1136/>	Scattered Spider threat actors create new user identities in the targeted organization.
Modify Authentication Process: Multi-Factor Authentication	T1556.006 <https://attack.mitre.org/versions/v14/techniques/t1556/006/>	Scattered Spider threat actors may modify MFA tokens to gain access to a victim's network.

Technique Title	ID	Use
Valid Accounts	T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>	Scattered Spider threat actors abuse and control valid accounts to maintain network access even when passwords are changed.

Table 9: Privilege Escalation

Technique Title	ID	Use
Privilege Escalation	TA0004 <https://attack.mitre.org/versions/v14/tactics/ta0004/>	Scattered Spider threat actors escalate account privileges when on a targeted organization's network.
Domain Policy Modification: Domain Trust Modification	T1484.002 <https://attack.mitre.org/versions/v14/techniques/t1484/002/>	Scattered Spider threat actors add a federated identify provider to the victim's SSO tenant and activate automatic account linking.

Table 10: Defense Evasion

Technique Title	ID	Use

Technique Title	ID	Use
Modify Cloud Compute Infrastructure: Create Cloud Instance	T1578.002 <https://attack.mitre.org/versions/v14/techniques/t1578/002/>	Scattered Spider threat actors will create cloud instances for use during lateral movement and data collection.
Impersonation	TA1656 <https://attack.mitre.org/versions/v14/techniques/t1656/>	Scattered Spider threat actors pose as company IT and/or helpdesk staff to gain access to victim's networks. Scattered Spider threat actors use social engineering to convince IT help desk personnel to reset passwords and/or MFA tokens.

Table 11: Credential Access

Technique Title	ID	Use
Credential Access	TA0006 <https://attack.mitre.org/versions/v14/tactics/ta0006/>	Scattered Spider threat actors use tools, such as Raccoon Stealer, to obtain login credentials.

Technique Title	ID	Use
Forge Web Credentials	T1606 <https://attack.mitre.org/versions/v14/techniques/t1606/>	Scattered Spider threat actors may forge MFA tokens to gain access to a victim's network.
Multi-Factor Authentication Request Generation	T1621 <https://attack.mitre.org/versions/v14/techniques/t1621/>	Scattered Spider sends repeated MFA notification prompts to lead employees to accept the prompt and gain access to the target network.
Unsecured Credentials: Credentials in Files	T1552.001 <https://attack.mitre.org/versions/v14/techniques/t1552/001/>	Scattered Spider threat actors search for insecurely stored credentials on victim's systems.
Unsecured Credentials: Private Keys	T1552.004 <https://attack.mitre.org/versions/v14/techniques/t1552/004/>	Scattered Spider threat actors search for insecurely stored private keys on victim's systems.

Table 12: Discovery

Technique Title	ID	Use

Technique Title	**ID**	**Use**
Discovery	TA0007 <https://attack.mitre.org/versions/v14/tactics/ta0007/>	Upon gaining access to a targeted network, Scattered Spider threat actors seek out SharePoint sites, credential storage documentation, VMware vCenter, infrastructure backups and enumerate AD to identify useful information to support further operations.
Browser Information Discovery	T1217 <https://attack.mitre.org/versions/v14/techniques/t1217/>	Scattered Spider threat actors use tools (e.g., Raccoon Stealer) to obtain browser histories.
Cloud Service Dashboard	T1538 <https://attack.mitre.org/versions/v14/techniques/t1538/>	Scattered Spider threat actors leverage AWS Systems Manager Inventory to discover targets for lateral movement.
File and Directory Discovery	T1083 <https://attack.mitre.org/versions/v14/techniques/t1083/>	Scattered Spider threat actors search a compromised network to discover files and directories for further information or exploitation.
Remote System Discovery	T1018 <https://attack.mitre.org/versions/v14/techniques/t1018/>	Scattered Spider threat actors search for infrastructure, such as remote systems, to exploit.

Technique Title	ID	Use
Steal Web Session Cookie	T1539 <https://attack.mitre.org/versions/v14/techniques/t1539/>	Scattered Spider threat actors use tools, such as Raccoon Stealer, to obtain browser cookies.

Table 13: Lateral Movement

Technique Title	ID	Use
Lateral Movement	TA0008 <https://attack.mitre.org/versions/v14/tactics/ta0008/>	Scattered Spider threat actors laterally move across a target network upon gaining access and establishing persistence.
Remote Services: Cloud Services	T1021.007 <https://attack.mitre.org/versions/v14/techniques/t1021/007/>	Scattered Spider threat actors use pre-existing cloud instances for lateral movement and data collection.

Table 14: Collection

Technique Title	ID	Use
Data from Information Repositories: Code Repositories	T1213.003 <https://attack.mitre.org/versions/v14/techniques/t1213/003/.003>	Scattered Spider threat actors search code repositories for data collection and exfiltration.

Technique Title	ID	Use
Data from Information Repositories: Sharepoint	T1213.002 <https://attack.mitre.org/versions/v14/techniques/t1213/002/>	Scattered Spider threat actors search SharePoint repositories for information.
Data Staged	T1074 <https://attack.mitre.org/versions/v14/techniques/t1074/>	Scattered Spider threat actors stage data from multiple data sources into a centralized database before exfiltration.
Email Collection	T1114 <https://attack.mitre.org/versions/v14/techniques/t1114/>	Scattered Spider threat actors search victim's emails to determine if the victim has detected the intrusion and initiated any security response.
Data from Cloud Storage	T1530 <https://attack.mitre.org/versions/v14/techniques/t1530/>	Scattered Spider threat actors search data in cloud storage for collection and exfiltration.

Table 15: Command and Control

Technique Title	ID	Use

Technique Title	ID	Use
Remote Access Software	T1219 <https://attack.mitre.org/versions/v14/techniques/t1219/>	Impersonating helpdesk personnel, Scattered Spider threat actors direct employees to run commercial remote access tools thereby enabling access to and command and control of the victim’s network. Scattered Spider threat actors leverage third-party software to facilitate lateral movement and maintain persistence on a target organization’s network.

Table 16: Exfiltration

Technique Title	ID	Use
Exfiltration	TA0010 <https://attack.mitre.org/versions/v14/tactics/ta0010/>	Scattered Spider threat actors exfiltrate data from a target network to for data extortion.

Table 17: Impact

Technique Title	ID	Use

Technique Title	ID	Use
Data Encrypted for Impact	T1486 <https://attack.mitre.org/versions/v14/techniques/t1486/>	Scattered Spider threat actors recently began encrypting data on a target network and demanding a ransom for decryption. Scattered Spider threat actors has been observed encrypting VMware ESXi servers.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002 <https://attack.mitre.org/versions/v14/techniques/t1567/002/>	Scattered Spider threat actors exfiltrate data to multiple sites including U.S.-based data centers and MEGA[.]NZ.
Financial Theft	T1657 <https://attack.mitre.org/versions/v14/techniques/t1657/>	Scattered Spider threat actors monetized access to victim networks in numerous ways including extortion-enabled ransomware and data theft.

MITIGATIONS

These mitigations apply to all critical infrastructure organizations and network defenders. The FBI and CISA recommend that software manufactures incorporate secure-by-design and -default principles and tactics into their software development practices limiting the impact of ransomware techniques, thus, strengthening the secure posture for their customers.

For more information on secure by design, see CISA's Secure by Design and Default <https://www.cisa.gov/securebydesign> webpage and joint guide <https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default>.

The FBI and CISA recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on the threat actor activity and to reduce the risk of compromise by Scattered Spider threat actors. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals <https://www.cisa.gov/cpg> for more information on the CPGs, including additional recommended baseline protections.

- **Implement application controls** to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.

- **Reduce threat of malicious actors** using remote access tools by:
  - **Auditing remote access tools** on your network to identify currently used and/or authorized software.
  - **Reviewing logs for execution of remote access software** to detect abnormal use of programs running as a portable executable [CPG 2.T </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
  - **Using security software** to detect instances of remote access software being loaded only in memory.
  - **Requiring authorized remote access solutions** to be used only from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
  - **Blocking both inbound and outbound connections** on common remote access software ports and protocols at the network perimeter.
  - **Applying recommendations** in the Guide to Securing Remote Access Software </sites/default/files/2023-06/guide%20to%20securing%20remote%20access%20software_clean%20final_508c.pdf>.
- **Implementing FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based MFA**. These MFA implementations are resistant to phishing and not suspectable to push bombing or SIM swap attacks, which are techniques known to be used by Scattered Spider actors. See CISA's fact sheet Implementing Phishing-Resistant MFA </sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf> for more information.

- **Strictly limit the use of Remote Desktop Protocol (RDP) and other remote desktop services**. If RDP is necessary, rigorously apply best practices, for example [CPG 2.W </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>]:
    - Audit the network for systems using RDP.
    - Close unused RDP ports.
    - Enforce account lockouts after a specified number of attempts.
    - Apply phishing-resistant multifactor authentication (MFA) </sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>.
    - Log RDP login attempts.

In addition, the authoring authorities of this CSA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- **Maintain offline backups of data** and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization limits the severity of disruption to its business practices [CPG 2.R </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with NIST's standards <https://pages.nist.gov/800-63-3/> for developing and managing password policies.
  - Implement password policies in compliance with NIST's standards.
  - Use "strong" passwords that are unique and random, as well as contain at least sixteen characters and no more than 64 characters in length [CPG 2.B <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
  - Consider implementing industry-recognized password managers that align with organizational technology procurement policies.
  - Avoid reusing passwords [CPG 2.C <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
  - Implement multiple failed login attempt account lockouts [CPG 2.G <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
  - Disable password "hints."
  - Refrain from requiring recurring password changes.
    Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
  - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication (MFA)** for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems [CPG 2.H </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> in internet-facing systems [CPG 1.E </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement [CPG 2.F </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic and activity, including lateral movement, on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host [CPG 3.A </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Disable unused ports and protocols** [CPG 2.V </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M </sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
- **Disable hyperlinks** in received emails.
- **Ensure all backup data is encrypted, immutable** (i.e., ensure backup data cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the FBI and CISA recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The FBI and CISA recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 4-17).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI and CISA recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REPORTING

The FBI and CISA are seeking any information that can be shared, to include a sample ransom note, communications with Scattered Spider group actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. The FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office <http://www.fbi.gov/contact-us/field-offices>, report the incident to the FBI Internet Crime Complaint Center (IC3) at IC3.gov <https://www.ic3.gov/>, or CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

REFERENCES

[1] MITRE ATT&CK – Scattered Spider <https://attack.mitre.org/versions/v14/groups/g1015/>

[2] Trellix - Scattered Spider: The Modus Operandi <https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html>

[3] Crowdstrike - Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies <https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/>

[4] Crowdstrike - SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-

Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security <https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/>

[5] Malwarebytes - Ransomware group steps up, issues statement over MGM Resorts compromise <https://www.malwarebytes.com/blog/personal/2023/09/ransomware-group-steps-up-issues-statement-over-mgm-resorts-compromise>

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The FBI and CISA do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI and CISA.

VERSION HISTORY

November 16, 2023: Initial version.
November 21, 2023: Updated password recommendation language on page 12.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

Topics: Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Malware, Phishing, and Ransomware </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Related Advisories

FEB 29, 2024 **CYBERSECURITY ADVISORY | AA24-060A**

#StopRansomware: Phobos Ransomware </news-events/cybersecurity-advisories/aa24-060a>

FEB 29, 2024 **CYBERSECURITY ADVISORY | AA24-060B**

Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways </news-events/cybersecurity-advisories/aa24-060b>

FEB 26, 2024 **CYBERSECURITY ADVISORY | AA24-057A**

SVR Cyber Actors Adapt Tactics for Initial Cloud Access </news-events/cybersecurity-advisories/aa24-057a>

FEB 15, 2024 **CYBERSECURITY ADVISORY | AA24-046A**

Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization </news-events/cybersecurity-advisories/aa24-046a>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

888-282-0870 central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility </accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Prevent Cyberattacks, Make Your Passwords Secure

PERSONAL TECHNOLOGY

NICOLE NGUYEN

I RECENTLY STAGED a password intervention.

One family member admitted to using the *same* password for every account. Another stored login credentials in iPhone Contacts. Both habits make accounts vulnerable to hackers. I had to step in.

Cyberattacks are more prevalent than ever.

Lucky for my sitting-duck family members, I've been on the receiving end of pro-grade cybersecurity advice for years. I set them up with a password manager, swapped out their weak passwords, turned on two-factor authentication and changed their device passcodes from "1111."

The great thing is, these updates made their digital lives safer *and* more convenient to access. If you need to stage an intervention on a family member—or even on yourself—use these four steps.

Set up a password manager

If you don't already have a password manager, it will take some work up front. But it's Step 1 for a reason, and the initial setup pains will make life easier. Your logins will automatically appear when you sign into a website. When creating new accounts on apps and websites, your manager will generate long and impossible-to-memorize passwords and save them for you.

I like these managers because they're built on what's called zero-knowledge architecture: The master password that secures your account isn't on company servers. No hacker or company employee could get to it. But also, the company can't recover it if you lose it.

Which means you have to come up with a good master password—and *remember* it. You can test its strength using Bitwarden's free (and secure) online checker. You're allowed to write it down on paper, if you store it in a safe place.

When picking a password manager, there are free and paid third-party options.

- **Free:** Bitwarden works across different browsers and operating systems. You can pay to upgrade—starting at $10 a year—if you want additional features such as family password sharing and trusted contacts for emergency access.
- **Paid:** I recommend 1Password ($3 a month for individuals, $5 for up to five accounts) for its balance of price and features. Many people also like Dashlane ($5 a month for individuals, $7.49 for up to 10 accounts), which includes a VPN for private internet browsing. Both are ideal for families. With a subscription, you can keep communal accounts (e.g. Netflix) in a shared "vault" and the apps can also monitor the web for exposed passwords, Social Security numbers and other data.

Once you've picked your password manager, download its app on every mobile device you own. On your computer, install the password manager's browser extension. In app settings, enable face or fingerprint authentication (on iPhones, that's Face ID or Touch ID) for easier access. Then, enable the manager to autofill logins.

If that sounds too complicated, you can use your device's free, built-in password manager.

Change reused passwords

Using the same password for many sites means a data breach on one exposes you on all the rest. Last month, genetic-testing company 23andMe reported that hackers accessed about 14,000 accounts because of password reuse.

Password managers can identify all your compromised, reused and weak passwords. 1Password offers a feature called Watchtower, Dashlane does dark-web monitoring, iCloud Keychain shows security recommendations and Google has a password checkup.

You can also check the secure website Have I Been Pwned to see if other types of data have been compromised.

The site was created by Troy Hunt, a security professional and director at Microsoft. Enter your email address, and the site combs publicly available data breaches. It will list services that exposed any usernames, passwords, phone numbers and more.

Two-factor authentication

Just like you have a deadbolt on your door, you need a "second factor" on your accounts. You can turn this on for major services in security settings—if they haven't already required you to.

The most basic second factor is a text message with a code, but it's not great. Technically, a criminal who really wants your account can steal your phone number from your carrier and redirect the codes.

An extreme option—but perhaps the safest—is a physical dongle called a security key, which you tap on your phone or plug into your computer.

The goldilocks choice is an authentication app. These spit out time-based codes tied to your account using cryptographic hocus-pocus.

I like Twilio's Authy because you can download it on multiple devices, which is a good backup plan if you lose one. Google Authenticator is another free option.

A new form of login—passkeys—ties passwords and two-factor authentication together in a convenient way. It's still in its early days, but you can try it in the security settings of your Google, Apple or Amazon accounts.

Secure your devices

Cyberattackers outnumber pickpockets, mostly because they can try to hack many victims at once. But a thief who steals your phone *and* your device passcode can do a lot of damage.

For one thing, the passcode can help an iPhone thief access the built-in iCloud Keychain password manager, which is why I think it's safer to use a third-party manager.

An iPhone feature called Stolen Device Protection, due to arrive soon in iOS 17.3, adds a layer of security to iCloud Keychain. But you have to turn it on when it arrives, or it does nothing.

That's why you also need to make sure the passcode on your iPhone or Android device is super secure, with numbers *and* letters if possible.

Also, consider a screen protector with a privacy filter. Add protective PINs to financial apps.

ILLUSTRATION: RACHEL MENDELSON/THE WALL STREET JOURNAL; ISTOCK (2)

Gmail **Jess Bunshaft <jess.bunshaft@gmail.com>**

Fwd: Vulnerability Summary for the Week of November 6, 2023

Ira Warshawsky <iwarshawsky45@gmail.com> Thu, Nov 16, 2023 at 5:06 PM
To: Jesse Bunshaft <jess.bunshaft@gmail.com>, Elizabeth.Daitz@suffolkcountyny.gov, bchou@gbgmatlaw.com, "tarver@tarverlawfirm.com" <tarver@tarverlawfirm.com>, torourke@bodnerorourke.com

---------- Forwarded message ---------
From: **CISA** <CISA@messages.cisa.gov>
Date: Thu, Nov 16, 2023 at 4:38 PM
Subject: Vulnerability Summary for the Week of November 6, 2023
To: <iwarshawsky45@gmail.com>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
DEFEND TODAY, SECURE TOMORROW

You are subscribed to Vulnerability Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of November 6, 2023

11/16/2023 04:00 PM EST

The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. NVD is sponsored by CISA. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Vulnerabilities are based on the Common Vulnerabilities and Exposures (CVE) vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- High: vulnerabilities with a CVSS base score of 7.0–10.0
- Medium: vulnerabilities with a CVSS base score of 4.0–6.9
- Low: vulnerabilities with a CVSS base score of 0.0–3.9

Entries may include additional information provided by organizations and efforts sponsored by CISA. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletin is compiled from external, open-source reports and is not a direct result of CISA analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1e -- platform	The 1E-Exchange-URLResponseTime instruction that is part of the Network product pack available on the 1E Exchange does not properly validate the URL parameter, which allows for a specially	2023-11-06	7.2	CVE-2023-45161 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crafted input to perform arbitrary code execution with SYSTEM permissions. To remediate this issue download the updated Network product pack from the 1E Exchange and update the 1E-Exchange-URLResponseTime instruction to v20.1 by uploading it through the 1E Platform instruction upload UI			
1e -- platform	The 1E-Exchange-CommandLinePing instruction that is part of the Network product pack available on the 1E Exchange does not properly validate the input parameter, which allows for a specially crafted input to perform arbitrary code execution with SYSTEM permissions. To remediate this issue download the updated Network product pack from the 1E Exchange and update the 1E-Exchange-CommandLinePing instruction to v18.1 by uploading it through the 1E Platform instruction upload UI	2023-11-06	7.2	CVE-2023-45163 MISC MISC
1e -- platform	The 1E-Exchange-DisplayMessageinstruction that is part of the End-User Interaction product pack available on the 1E Exchange does not properly validate the Caption or Message parameters, which allows for a specially crafted input to perform arbitrary code execution with SYSTEM permissions. To remediate this issue DELETE the instruction "Show dialogue with caption %Caption% and message %Message%" from the list of instructions in the Settings UI, and replace it with the new instruction 1E-Exchange-ShowNotification instruction available in the updated End-User Interaction product pack. The new instruction should show as "Show %Type% type notification with header %Header% and message %Message%" with a version of 7.1 or above.	2023-11-06	7.2	CVE-2023-5964 MISC MISC
7-zip -- 7-zip	7-Zip through 22.01 on Linux allows an integer underflow and code execution via a crafted 7Z archive.	2023-11-03	7.8	CVE-2023-31102 MISC MISC MISC
advanced_export_products_orders_cron_csv_excel_project -- advanced_export_products_orders_cron_csv_excel	Insecure permissions in Smart Soft advancedexport before v4.4.7 allow unauthenticated attackers to arbitrarily download user information from the ps_customer table.	2023-11-07	7.5	CVE-2023-43984
arm -- valhall_gpu_kernel_driver	A local non-privileged user can make improper GPU memory processing operations. If the operations are carefully prepared, then they could be used to gain access to already freed memory.	2023-11-07	7.8	CVE-2023-3889
arm -- valhall_gpu_kernel_driver	A local non-privileged user can make improper GPU memory processing operations to gain access to already freed memory.	2023-11-07	7.8	CVE-2023-4295
asus -- rt-ax55_firmware	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its token-generated module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system, or terminate services.	2023-11-03	8.8	CVE-2023-41345 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
asus -- rt-ax55_firmware	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its token-refresh module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	2023-11-03	8.8	CVE-2023-41346 MISC
asus -- rt-ax55_firmware	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its check token module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	2023-11-03	8.8	CVE-2023-41347 MISC
asus -- rt-ax55_firmware	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its code-authentication module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	2023-11-03	8.8	CVE-2023-41348 MISC
asus -- rt-ax57_firmware	An issue in ASUS RT-AX57 v.3.0.0.4_386_52041 allows a remote attacker to execute arbitrary code via a crafted request to the lan_ifname field in the sub_In 2C318 function.	2023-11-09	9.8	CVE-2023-47005
asus -- rt-ax57_firmware	An issue in ASUS RT-AX57 v.3.0.0.4_386_52041 allows a remote attacker to execute arbitrary code via a crafted request to the lan_ipaddr field in the sub_6FC74 function.	2023-11-09	9.8	CVE-2023-47006
asus -- rt-ax57_firmware	An issue in ASUS RT-AX57 v.3.0.0.4_386_52041 allows a remote attacker to execute arbitrary code via a crafted request to the lan_ifname field in the sub_391B8 function.	2023-11-09	9.8	CVE-2023-47007
asus -- rt-ax57_firmware	An issue in ASUS RT-AX57 v.3.0.0.4_386_52041 allows a remote attacker to execute arbitrary code via a crafted request to the ifname field in the sub_4CCE4 function.	2023-11-09	9.8	CVE-2023-47008
best_courier_management_system -- best_courier_management_system	An issue in Best Courier Management System v.1.0 allows a remote attacker to execute arbitrary code and escalate privileges via a crafted script to the userID parameter.	2023-11-03	9.8	CVE-2023-46980 MISC MISC
bestpractical -- request_tracker	Best Practical Request Tracker (RT) before 4.4.7 and 5.x before 5.0.5 allows Information Disclosure via fake or spoofed RT email headers in an email message or a mail-gateway REST API call.	2023-11-03	7.5	CVE-2023-41259 MISC CONFIRM CONFIRM
bestpractical -- request_tracker	Best Practical Request Tracker (RT) before 4.4.7 and 5.x before 5.0.5 allows Information Exposure in responses to mail-gateway REST API calls.	2023-11-03	7.5	CVE-2023-41260 MISC CONFIRM CONFIRM
bestpractical -- request_tracker	Best Practical Request Tracker (RT) 5 before 5.0.5 allows Information Disclosure via a transaction search in the transaction query builder.	2023-11-03	7.5	CVE-2023-45024 MISC CONFIRM
bleachbit -- bleachbit	BleachBit cleans files to free disk space and to maintain privacy. BleachBit for Windows up to version 4.4.2 is vulnerable to a DLL Hijacking	2023-11-08	7.3	CVE-2023-47113

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability. By placing a DLL in the Folder c:\DLLs, an attacker can run arbitrary code on every execution of BleachBit for Windows. This issue has been patched in version 4.5.0.			
boltwire -- boltwire	An issue in BoltWire v.6.03 allows a remote attacker to obtain sensitive information via a crafted payload to the view and change admin password function.	2023-11-07	9.1	CVE-2023-46501
botan_project -- botan	bcrypt password hashing in Botan before 2.1.0 does not correctly handle passwords with a length between 57 and 72 characters, which makes it easier for attackers to determine the cleartext password.	2023-11-03	7.5	CVE-2017-7252 CONFIRM MISC
clickbar -- dot-diver	Dot diver is a lightweight, powerful, and dependency-free TypeScript utility library that provides types and functions to work with object paths in dot notation. In versions prior to 1.0.2 there is a Prototype Pollution vulnerability in the `setByPath` function which can leads to remote code execution (RCE). This issue has been addressed in commit `98daf567` which has been included in release 1.0.2. Users are advised to upgrade. There are no known workarounds to this vulnerability.	2023-11-06	9.8	CVE-2023-45827 MISC MISC
couchbase -- couchbase_server	Couchbase Server 7.1.4 before 7.1.5 and 7.2.0 before 7.2.1 allows Directory Traversal.	2023-11-08	7.5	CVE-2023-36667
djangoproject -- django	In Django 3.2 before 3.2.21, 4.1 before 4.1.11, and 4.2 before 4.2.5, django.utils.encoding.uri_to_iri() is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.	2023-11-03	7.5	CVE-2023-41164 CONFIRM MISC
djangoproject -- django	In Django 3.2 before 3.2.22, 4.1 before 4.1.12, and 4.2 before 4.2.6, the django.utils.text.Truncator chars() and words() methods (when used with html=True) are subject to a potential DoS (denial of service) attack via certain inputs with very long, potentially malformed HTML text. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which are thus also vulnerable. NOTE: this issue exists because of an incomplete fix for CVE-2019-14232.	2023-11-03	7.5	CVE-2023-43665 CONFIRM MISC
ec-cube -- ec-cube	EC-CUBE 3 series (3.0.0 to 3.0.18-p6) and 4 series (4.0.0 to 4.0.6-p3, 4.1.0 to 4.1.2-p2, and 4.2.0 to 4.2.2) contain an arbitrary code execution vulnerability due to improper settings of the template engine Twig included in the product. As a result, arbitrary code may be executed on the server where the product is running by a user with an administrative privilege.	2023-11-07	7.2	CVE-2023-46845
eclipse -- glassfish	In Eclipse Glassfish 5 or 6, running with old versions of JDK (lower than 6u211, or < 7u201, or < 8u191), allows remote attackers to load malicious code on the server via access to insecure ORB listeners.	2023-11-03	9.8	CVE-2023-5763 MISC MISC
eclipse -- parsson	In Eclipse Parsson before versions 1.1.4 and 1.0.5, Parsing JSON from untrusted sources can lead malicious actors to exploit the fact that the	2023-11-03	7.5	CVE-2023-4043 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	built-in support for parsing numbers with large scale in Java has a number of edge cases where the input text of a number can lead to much larger processing time than one would expect. To mitigate the risk, parsson put in place a size limit for the numbers as well as their scale.			
espressif -- esptool	An issue discovered in esptool 4.6.2 allows attackers to view sensitive information via weak cryptographic algorithm.	2023-11-09	7.5	CVE-2023-46894
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Alex Raven WP Report Post plugin <= 2.1.2 versions.	2023-11-09	8.8	CVE-2023-34171
exiv2 -- exiv2	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. An out-of-bounds write was found in Exiv2 version v0.28.0. The vulnerable function, `BmffImage::brotliUncompress`, is new in v0.28.0, so earlier versions of Exiv2 are _not_ affected. The out-of-bounds write is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. This bug is fixed in version v0.28.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-11-06	8.8	CVE-2023-44398 MISC MISC
felixwelberg -- sis_handball	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Felix Welberg SIS Handball allows SQL Injection.This issue affects SIS Handball: from n/a through 1.0.45.	2023-11-06	9.8	CVE-2023-33924 MISC
froxlor -- froxlor	Improper Input Validation in GitHub repository froxlor/froxlor prior to 2.1.0.	2023-11-10	8.8	CVE-2023-6069
frrouting -- frrouting	bgpd/bgp_flowspec.c in FRRouting (FRR) before 8.4.3 mishandles an nlri length of zero, aka a "flowspec overflow."	2023-11-06	9.8	CVE-2023-38406 MISC MISC
frrouting -- frrouting	bgpd/bgp_label.c in FRRouting (FRR) before 8.5 attempts to read beyond the end of the stream during labeled unicast parsing.	2023-11-06	7.5	CVE-2023-38407 MISC MISC MISC
frrouting -- frrouting	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur when processing a crafted BGP UPDATE message with a MP_UNREACH_NLRI attribute and additional NLRI data (that lacks mandatory path attributes).	2023-11-03	7.5	CVE-2023-47234 MISC
frrouting -- frrouting	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur when a malformed BGP UPDATE message with an EOR is processed, because the presence of EOR does not lead to a treat-as-withdraw outcome.	2023-11-03	7.5	CVE-2023-47235 MISC
ge -- micom_s1_agile	General Electric MiCOM S1 Agile is vulnerable to an attacker achieving code execution by placing malicious DLL files in the directory of the application.	2023-11-07	7.3	CVE-2023-0898
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 11.6 before	2023-11-06	7.7	CVE-2023-3399 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1. It was possible for an unauthorised project or group member to read the CI/CD variables using the custom project templates.			MISC
google -- android	In video, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08235273; Issue ID: ALPS08250357.	2023-11-06	7.8	CVE-2023-32837 MISC
google -- android	In video, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08235273; Issue ID: ALPS08235273.	2023-11-06	7	CVE-2023-32832 MISC
google -- chrome	Use after free in WebAudio in Google Chrome prior to 119.0.6045.123 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-08	8.8	CVE-2023-5996
gpac -- gpac	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3.0-DEV.	2023-11-07	7.5	CVE-2023-5998
group-office -- group_office	Group-Office is an enterprise CRM and groupware tool. In affected versions there is full Server-Side Request Forgery (SSRF) vulnerability in the /api/upload.php endpoint. The /api/upload.php endpoint does not filter URLs which allows a malicious user to cause the server to make resource requests to untrusted domains. Note that protocols like file:// can also be used to access the server disk. The request result (on success) can then be retrieved using /api/download.php. This issue has been addressed in versions 6.8.15, 6.7.54, and 6.6.177. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-11-07	8.8	CVE-2023-46730
gss -- vitals_enterprise_social_platform	Galaxy Software Services Corporation Vitals ESP is an online knowledge base management portal, it has insufficient filtering and validation during file upload. An authenticated remote attacker with general user privilege can exploit this vulnerability to upload and execute scripts onto arbitrary directories to perform arbitrary system operations or disrupt service.	2023-11-03	8.8	CVE-2023-41357 MISC
huawei -- emui	Vulnerability of missing encryption in the card management module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	CVE-2023-44098
huawei -- emui	Vulnerability of uncaught exceptions in the NFC module. Successful exploitation of this vulnerability can affect NFC availability.	2023-11-08	7.5	CVE-2023-46765
huawei -- emui	Security vulnerability in the face unlock module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	CVE-2023-46771
huawei -- emui	Vulnerability of uncaught exceptions in the NFC module. Successful exploitation of this vulnerability can affect NFC availability.	2023-11-08	7.5	CVE-2023-46774

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- harmonyos	Vulnerability of identity verification being bypassed in the face unlock module. Successful exploitation of this vulnerability will affect integrity and confidentiality.	2023-11-08	9.1	CVE-2023-5801
huawei -- harmonyos	Vulnerability of improper permission control in the Booster module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	CVE-2023-44115
huawei -- harmonyos	The remote PIN module has a vulnerability that causes incorrect information storage locations.Successful exploitation of this vulnerability may affect confidentiality.	2023-11-08	7.5	CVE-2023-46757
huawei -- harmonyos	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device.	2023-11-08	7.5	CVE-2023-46758
huawei -- harmonyos	Permission control vulnerability in the call module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	CVE-2023-46759
huawei -- harmonyos	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	CVE-2023-46760
huawei -- harmonyos	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	CVE-2023-46761
huawei -- harmonyos	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	CVE-2023-46762
huawei -- harmonyos	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	CVE-2023-46766
huawei -- harmonyos	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	CVE-2023-46767
huawei -- harmonyos	Multi-thread vulnerability in the idmap module. Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-11-08	7.5	CVE-2023-46768
huawei -- harmonyos	Use-After-Free (UAF) vulnerability in the dubai module. Successful exploitation of this vulnerability will affect availability.	2023-11-08	7.5	CVE-2023-46769
huawei -- harmonyos	Out-of-bounds vulnerability in the sensor module. Successful exploitation of this vulnerability may cause mistouch prevention errors on users' mobile phones.	2023-11-08	7.5	CVE-2023-46770
ibm -- cics_tx	IBM CICS TX Standard 11.1 and Advanced 10.1, 11.1 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 266163.	2023-11-03	7.5	CVE-2023-43018 MISC MISC
ibm -- mq_appliance	IBM MQ Appliance 9.3 CD could allow a local attacker to gain elevated privileges on the system, caused by improper validation of security keys. IBM X-Force ID: 269535.	2023-11-03	7.8	CVE-2023-46176 MISC MISC
ibm -- txseries_for_multiplatforms	IBM CICS TX Standard 11.1, Advanced 10.1, 11.1, and TXSeries for Multiplatforms 8.1, 8.2, 9.1 are vulnerable to cross-site request forgery which	2023-11-03	8.8	CVE-2023-42027 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 266057.			MISC MISC
intelliants -- subrion	Subrion 4.2.1 has a remote command execution vulnerability in the backend.	2023-11-03	8.8	CVE-2023-46947 MISC
ivanti -- automation	A locally authenticated attacker with low privileges can bypass authentication due to insecure inter-process communication.	2023-11-03	7.8	CVE-2022-44569 MISC
ivanti -- avalanche	Ivanti Avalanche Smart Device Service Missing Authentication Local Privilege Escalation Vulnerability	2023-11-03	7.8	CVE-2022-43554 MISC
ivanti -- avalanche	Ivanti Avalanche Printer Device Service Missing Authentication Local Privilege Escalation Vulnerability	2023-11-03	7.8	CVE-2022-43555 MISC
ivanti -- avalanche	Ivanti Avalanche EnterpriseServer Service Unrestricted File Upload Local Privilege Escalation Vulnerability	2023-11-03	7.8	CVE-2023-41725 MISC
ivanti -- avalanche	Ivanti Avalanche Incorrect Default Permissions allows Local Privilege Escalation Vulnerability	2023-11-03	7.8	CVE-2023-41726 MISC
kerawen -- kerawen	kerawen before v2.5.1 was discovered to contain a SQL injection vulnerability via the ocs_id_cart parameter at KerawenDeliveryModuleFrontController::initContent().	2023-11-04	9.8	CVE-2023-40922 MISC
kubernetes -- apiserver	A security issue was discovered in kube-apiserver that allows an aggregated API server to redirect client traffic to any URL. This could lead to the client performing unexpected actions as well as forwarding the client's API server credentials to third parties.	2023-11-03	8.2	CVE-2022-3172 MISC MISC
kubernetes -- csi_proxy	A security issue was discovered in Kubernetes where a user that can create pods on Windows nodes running kubernetes-csi-proxy may be able to escalate to admin privileges on those nodes. Kubernetes clusters are only affected if they include Windows nodes running kubernetes-csi-proxy.	2023-11-03	8.8	CVE-2023-3893 MISC MISC
kyocera -- d-copia253mf_plus_firmware	Kyocera TASKalfa 4053ci printers through 2VG_S000.002.561 allow a denial of service (service outage) via /wlmdeu%2f%2e%2e%2f%2e%2e followed by a directory reference such as %2fetc%00index.htm to try to read the /etc directory.	2023-11-03	7.5	CVE-2023-34260 MISC MISC
linagora -- twake	Improper Restriction of Excessive Authentication Attempts in GitHub repository linagora/twake prior to 2023.Q1.1223.	2023-11-07	9.8	CVE-2023-2675
linux -- kernel	An out-of-bounds (OOB) memory read flaw was found in parse_lease_state in the KSMBD implementation of the in-kernel samba server and CIFS in the Linux kernel. When an attacker sends the CREATE command with a malformed payload to KSMBD, due to a missing check of \`NameOffset\` in the \`parse_lease_state()\` function, the \`create_context\` object can access invalid memory.	2023-11-03	8.1	CVE-2023-1194 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- kernel	A use-after-free flaw was found in the Linux kernel's mm/mremap memory address space accounting source code. This issue occurs due to a race condition between rmap walk and mremap, allowing a local user to crash the system or potentially escalate their privileges on the system.	2023-11-03	7	CVE-2023-1476 MISC MISC MISC MISC
lost_and_found_information_system -- lost_and_found_information_system	Lost and Found Information System 1.0 allows account takeover via username and password to a /classes/Users.php?f=save URI.	2023-11-03	9.8	CVE-2023-38965 MISC MISC
macvim -- macvim	Macvim is a text editor for MacOS. Prior to version 178, Macvim makes use of an insecure interprocess communication (IPC) mechanism which could lead to a privilege escalation. Distributed objects are a concept introduced by Apple which allow one program to vend an interface to another program. What is not made clear in the documentation is that this service can vend this interface to any other program on the machine. The impact of exploitation is a privilege escalation to root - this is likely to affect anyone who is not careful about the software they download and use MacVim to edit files that would require root privileges. Version 178 contains a fix for this issue.	2023-11-07	7.8	CVE-2023-41036
mediatek -- nr15	In 5G NRLC, there is a possible invalid memory access due to lack of error handling. This could lead to remote denial of service, if UE received invalid 1-byte rlc sdu, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00921261; Issue ID: MOLY01128895.	2023-11-06	7.5	CVE-2023-20702 MISC
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2023-11-10	7.3	CVE-2023-36014
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2023-11-03	7.3	CVE-2023-36034 MISC
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-11-10	7.1	CVE-2023-36024
midori-global -- better_pdf_exporter	Local File Inclusion vulnerability in Midori-global Better PDF Exporter for Jira Server and Jira Data Center v.10.3.0 and before allows an attacker to view arbitrary files and cause other impacts via use of crafted image during PDF export.	2023-11-07	7.8	CVE-2023-42361
mitsubishi_electric -- fx3u-32mt/es_firmware	Insufficient Verification of Data Authenticity vulnerability in Mitsubishi Electric Corporation MELSEC-F Series main modules and MELSEC iQ-F Series CPU modules allows a remote unauthenticated attacker to reset the memory of the products to factory default state and cause denial-of-service (DoS) condition on the products by sending specific packets.	2023-11-06	9.1	CVE-2023-4699 MISC MISC MISC
mongodb -- atlas_kubernetes_operator	The affected versions of MongoDB Atlas Kubernetes Operator may print sensitive information like GCP service account keys and API integration secrets while DEBUG mode logging is enabled. This issue affects MongoDB Atlas Kubernetes Operator versions: 1.5.0, 1.6.0, 1.6.1, 1.7.0. Please note that this is reported on an EOL	2023-11-07	7.5	CVE-2023-0436

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version of the product, and users are advised to upgrade to the latest supported version. Required Configuration: DEBUG logging is not enabled by default, and must be configured by the end-user. To check the log-level of the Operator, review the flags passed in your deployment configuration (eg. https://github.com/mongodb/mongodb-atlas-kubernetes/blob/main/config/manager/manager.yaml#L27 https://github.com/mongodb/mongodb-atlas-kubernetes/blob/main/config/manager/manager.yaml#L27)			
nationaledtech -- boomerang	An issue was discovered in the Boomerang Parental Control application through 13.83 for Android. The child can use Safe Mode to remove all restrictions temporarily or uninstall the application without the parents noticing.	2023-11-03	9.1	CVE-2023-36621 MISC MISC MISC
ncsist -- mobile_device_manager	NCSIST ManageEngine Mobile Device Manager(MDM) APP's special function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and read arbitrary system files.	2023-11-03	7.5	CVE-2023-41344 MISC
netskope -- netskope	Netskope was made aware of a security vulnerability in its NSClient product for version 100 & prior where a malicious non-admin user can disable the Netskope client by using a specially crafted package. The root cause of the problem was a user control code when called by a Windows ServiceController did not validate the permissions associated with the user before executing the user control code. This user control code had permissions to terminate the NSClient service.	2023-11-06	8.8	CVE-2023-4996 MISC
nokia -- g-040w-q_firmware	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of insufficient measures to prevent multiple failed authentication attempts. An unauthenticated remote attacker can execute a crafted Javascript to expose captcha in page, making it very easy for bots to bypass the captcha check and more susceptible to brute force attacks.	2023-11-03	9.8	CVE-2023-41350 MISC
nokia -- g-040w-q_firmware	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of authentication bypass, which allows an unauthenticated remote attacker to bypass the authentication mechanism to log in to the device by an alternative URL. This makes it possible for unauthenticated remote attackers to log in as any existing users, such as an administrator, to perform arbitrary system operations or disrupt service.	2023-11-03	9.8	CVE-2023-41351 MISC
nokia -- g-040w-q_firmware	Chunghwa Telecom NOKIA G-040W-Q Firewall function has a vulnerability of input validation for ICMP redirect messages. An unauthenticated remote attacker can exploit this vulnerability by sending a crafted package to modify the network routing table, resulting in a denial of service or sensitive information leaking.	2023-11-03	9.8	CVE-2023-41355 MISC
nokia -- g-040w-q_firmware	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of weak password requirements. A remote attacker with regular user privilege can easily infer the administrator password from system information after logging system, resulting	2023-11-03	8.8	CVE-2023-41353 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in admin access and performing arbitrary system operations or disrupt service.			
nokia -- g-040w-q_firmware	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of insufficient filtering for user input. A remote attacker with administrator privilege can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	2023-11-03	7.2	CVE-2023-41352 MISC
opayweb -- opay	An Information Disclosure vulnerability exists in Opay Mobile application 1.5.1.26 and maybe be higher in the logcat app.	2023-11-07	7.5	CVE-2021-43419
opendesign -- drawings_sdk	An issue was discovered in Open Design Alliance Drawings SDK before 2024.10. A corrupted value for the start of MiniFat sector in a crafted DGN file leads to an out-of-bounds read. This can allow attackers to cause a crash, potentially enabling a denial-of-service attack (Crash, Exit, or Restart) or possible code execution.	2023-11-07	7.8	CVE-2023-5179
openssl -- openssl	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.	2023-11-06	7.5	CVE-2023-5678 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ortussolutions -- coldbox_elixir	A vulnerability classified as problematic has been found in Ortus Solutions ColdBox Elixir 3.1.6. This affects an unknown part of the file src/defaultConfig.js of the component ENV Variable Handler. The manipulation leads to information disclosure. Upgrading to version 3.1.7 is able to address this issue. The identifier of the patch is a3aa62daea2e44c76d08d1eac63768 cd928cd69e. It is recommended to upgrade the affected component. The identifier VDB-244485 was assigned to this vulnerability.	2023-11-06	7.5	CVE-2021-4430 MISC MISC MISC MISC
perforce -- helix_core	An arbitrary code execution which results in privilege escalation was discovered in Helix Core versions prior to 2023.2. Reported by Jason Geffner.	2023-11-08	9.8	CVE-2023-45849
perforce -- helix_core	In Helix Core versions prior to 2023.2, an unauthenticated remote Denial of Service (DoS) via the shutdown function was identified. Reported by Jason Geffner.	2023-11-08	7.5	CVE-2023-35767
perforce -- helix_core	In Helix Core versions prior to 2023.2, an unauthenticated remote Denial of Service (DoS) via the commit function was identified. Reported by Jason Geffner.	2023-11-08	7.5	CVE-2023-45319
perforce -- helix_core	In Helix Core versions prior to 2023.2, an unauthenticated remote Denial of Service (DoS) via the buffer was identified. Reported by Jason Geffner.	2023-11-08	7.5	CVE-2023-5759
phpfox -- phpfox	An issue was discovered in phpFox before 4.8.14. The url request parameter passed to the /core/redirect route is not properly sanitized before being used in a call to the unserialize() PHP function. This can be exploited by remote, unauthenticated attackers to inject arbitrary PHP objects into the application scope, allowing them to perform a variety of attacks, such as executing arbitrary PHP code.	2023-11-03	9.8	CVE-2023-46817 MISC MISC MISC MISC MISC
prestashop-- prestashop	In the module "Order Duplicator " Clone and Delete Existing Order" (orderduplicate) in version <= 1.1.7 from Silbersaiten for PrestaShop, a guest can download personal information without restriction. Due to a lack of permissions control, a guest can download personal information from ps_customer/ps_address tables such as name / surname / phone number / full postal address.	2023-11-07	8.8	CVE-2023-45380
progress -- ws_ftp_server	In WS_FTP Server versions prior to 8.7.6 and 8.8.4, an unrestricted file upload flaw has been identified. An authenticated Ad Hoc Transfer user has the ability to craft an API call which allows them to upload a file to a specified location on the underlying operating system hosting the WS_FTP Server application.	2023-11-07	8.8	CVE-2023-42659
projectworlds -- online_job_portal	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txt_password' parameter of the index.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	9.8	CVE-2023-46680
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the	2023-11-07	9.8	CVE-2023-46785

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	partner_preference.php resource does not validate the characters received and they are sent unfiltered to the database.			
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'pass' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	9.8	CVE-2023-46798
puppet -- puppet_enterprise	Versions of Puppet Enterprise prior to 2021.7.6 and 2023.5 contain a flaw which results in broken session management for SAML implementations.	2023-11-07	9.8	CVE-2023-5309
python -- pillow	An issue was discovered in Pillow before 10.0.0. It is a Denial of Service that uncontrollably allocates memory to process a given task, potentially causing a service to crash by having it run out of memory. This occurs for truetype in ImageFont when textlength in an ImageDraw instance operates on a long text argument.	2023-11-03	7.5	CVE-2023-44271 MISC MISC MISC
qemu -- qemu	A bug in QEMU could cause a guest I/O operation otherwise addressed to an arbitrary disk offset to be targeted to offset 0 instead (potentially overwriting the VM's boot code). This could be used, for example, by L2 guests with a virtual disk (vdiskL2) stored on a virtual disk of an L1 (vdiskL1) hypervisor to read and/or write data to LBA 0 of vdiskL1, potentially gaining control of L1 at its next reboot.	2023-11-03	7	CVE-2023-5088 MISC MISC MISC
qnap -- music_station	A path traversal vulnerability has been reported to affect Music Station. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: Music Station 4.8.11 and later Music Station 5.1.16 and later Music Station 5.3.23 and later	2023-11-03	7.5	CVE-2023-39299 MISC
qnap -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2376 build 20230421 and later QTS 4.5.4.2374 build 20230416 and later QuTS hero h5.0.1.2376 build 20230421 and later QuTS hero h4.5.4.2374 build 20230417 and later QuTScloud c5.0.1.2374 and later	2023-11-03	9.8	CVE-2023-23368 MISC
qnap -- qts	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: Multimedia Console 2.1.2 (2023/05/04) and later Multimedia Console 1.4.8 (2023/05/05) and later QTS 5.1.0.2399 build 20230515 and later QTS 4.3.6.2441 build 20230621 and later QTS 4.3.4.2451 build 20230621 and later QTS 4.3.3.2420 build 20230621 and later QTS 4.2.6 build 20230621 and later Media Streaming add-on 500.1.1.2 (2023/06/12) and later Media	2023-11-03	9.8	CVE-2023-23369 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Streaming add-on 500.0.0.11 (2023/06/16) and later			
qualcomm -- snapdragon	Memory Corruption in Multi-mode Call Processor while processing bit mask API.	2023-11-07	9.8	CVE-2023-22388
qualcomm -- snapdragon	Memory corruption in WLAN Firmware while parsing a NAN management frame carrying a S3 attribute.	2023-11-07	9.8	CVE-2023-33045
qualcomm -- snapdragon	Memory corruption in WLAN HOST while processing the WLAN scan descriptor list.	2023-11-07	8.8	CVE-2023-28572
qualcomm -- snapdragon	Memory Corruption in Core during syscall for Sectools Fuse comparison feature.	2023-11-07	7.8	CVE-2023-21671
qualcomm -- snapdragon	Memory Corruption in Core due to secure memory access by user while loading modem image.	2023-11-07	7.8	CVE-2023-24852
qualcomm -- snapdragon	Memory corruption in TZ Secure OS while loading an app ELF.	2023-11-07	7.8	CVE-2023-28545
qualcomm -- snapdragon	Cryptographic issue in HLOS during key management.	2023-11-07	7.8	CVE-2023-28556
qualcomm -- snapdragon	Memory corruption while processing audio effects.	2023-11-07	7.8	CVE-2023-28570
qualcomm -- snapdragon	Memory corruption in core services when Diag handler receives a command to configure event listeners.	2023-11-07	7.8	CVE-2023-28574
qualcomm -- snapdragon	Memory corruption in Automotive Audio while copying data from ADSP shared buffer to the VOC packet data buffer.	2023-11-07	7.8	CVE-2023-33031
qualcomm -- snapdragon	Memory Corruption in Audio while invoking callback function in driver from ADSP.	2023-11-07	7.8	CVE-2023-33055
qualcomm -- snapdragon	Memory corruption in Audio while processing the VOC packet data from ADSP.	2023-11-07	7.8	CVE-2023-33059
qualcomm -- snapdragon	Memory corruption in Audio when SSR event is triggered after music playback is stopped.	2023-11-07	7.8	CVE-2023-33074
qualcomm -- snapdragon	Transient DOS in WLAN Firmware while parsing no-inherit IES.	2023-11-07	7.5	CVE-2023-33047
qualcomm -- snapdragon	Transient DOS in WLAN Firmware while parsing t2lm buffers.	2023-11-07	7.5	CVE-2023-33048
qualcomm -- snapdragon	Transient DOS in WLAN Firmware when firmware receives beacon including T2LM IE.	2023-11-07	7.5	CVE-2023-33056
qualcomm -- snapdragon	Transient DOS in WLAN Firmware while parsing WLAN beacon or probe-response frame.	2023-11-07	7.5	CVE-2023-33061
qualitor -- qalitor	Qualitor through 8.20 allows remote attackers to execute arbitrary code via PHP code in the html/ad/adpesquisasql/request/processVariavel.php gridValoresPopHidden parameter.	2023-11-06	9.8	CVE-2023-47253 MISC MISC MISC MISC
redlion -- crimson	The Crimson 3.2 Windows-based configuration tool allows users with administrative access to define new passwords for users and to download the resulting security configuration to a device. If such a password contains the percent (%) character, invalid values will be included, potentially truncating the string if a NUL is encountered. If the simplified password is not detected by the administrator, the device might be left in a vulnerable state as a result of more-easily	2023-11-06	9.8	CVE-2023-5719 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	compromised credentials. Note that passwords entered via the Crimson system web server do not suffer from this vulnerability.			
relativity -- relativityone	SQL Injection vulnerability in Relativity ODA LLC RelativityOne v.12.1.537.3 Patch 2 and earlier allows a remote attacker to execute arbitrary code via the name parameter.	2023-11-03	9.8	CVE-2023-46954 MISC
remoteclinic -- remote_clinic	RemoteClinic 2.0 has a SQL injection vulnerability in the ID parameter of /medicines/stocks.php.	2023-11-07	9.8	CVE-2023-33478
remoteclinic -- remote_clinic	RemoteClinic version 2.0 contains a SQL injection vulnerability in the /staff/edit.php file.	2023-11-07	9.8	CVE-2023-33479
remoteclinic -- remote_clinic	RemoteClinic 2.0 is vulnerable to a time-based blind SQL injection attack in the 'start' GET parameter of patients/index.php.	2023-11-07	9.8	CVE-2023-33481
remoteclinic -- remote_clinic	RemoteClinic 2.0 contains a critical vulnerability chain that can be exploited by a remote attacker with low-privileged user credentials to create admin users, escalate privileges, and execute arbitrary code on the target system via a PHP shell. The vulnerabilities are caused by a lack of input validation and access control in the staff/register.php endpoint and the edit-my-profile.php page. By sending a series of specially crafted requests to the RemoteClinic application, an attacker can create admin users with more privileges than their own, upload a PHP file containing arbitrary code, and execute arbitrary commands via the PHP shell.	2023-11-07	8.8	CVE-2023-33480
samba -- samba	A path traversal vulnerability was identified in Samba when processing client pipe names connecting to Unix domain sockets within a private directory. Samba typically uses this mechanism to connect SMB clients to remote procedure call (RPC) services like SAMR LSA or SPOOLSS, which Samba initiates on demand. However, due to inadequate sanitization of incoming client pipe names, allowing a client to send a pipe name containing Unix directory traversal characters (../). This could result in SMB clients connecting as root to Unix domain sockets outside the private directory. If an attacker or client managed to send a pipe name resolving to an external service using an existing Unix domain socket, it could potentially lead to unauthorized access to the service and consequential adverse events, including compromise or service crashes.	2023-11-03	9.8	CVE-2023-3961 MISC MISC MISC MISC MISC MISC
samsung -- android	Improper access control vulnerability in SmsController prior to SMR Nov-2023 Release1 allows attacker to bypass restrictions on starting activities from the background.	2023-11-07	9.8	CVE-2023-42531
samsung -- android	An improper input validation in saped_dec in libsaped prior to SMR Nov-2023 Release 1 allows attacker to cause out-of-bounds read and write.	2023-11-07	9.8	CVE-2023-42536
samsung -- android	An improper input validation in get_head_crc in libsaped prior to SMR Nov-2023 Release 1 allows attacker to cause out-of-bounds read and write.	2023-11-07	9.8	CVE-2023-42537
samsung -- android	An improper input validation in saped_rec_silence in libsaped prior to SMR Nov-2023 Release 1	2023-11-07	9.8	CVE-2023-42538

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows attacker to cause out-of-bounds read and write.			
samsung -- android	Arbitrary File Descriptor Write vulnerability in libsec-ril prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	2023-11-07	7.8	CVE-2023-30739
samsung -- android	Improper Input Validation vulnerability in ProcessNvBuffering of libsec-ril prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	2023-11-07	7.8	CVE-2023-42528
samsung -- android	Out-of-bound write vulnerability in libsec-ril prior to SMR Nov-2023 Release 1 allows local attackers to execute arbitrary code.	2023-11-07	7.8	CVE-2023-42529
samsung -- android	Out-of-bounds Write in read_block of vold prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	2023-11-07	7.8	CVE-2023-42535
samsung -- android	Improper access control vulnerability in SecSettings prior to SMR Nov-2023 Release 1 allows attackers to enable Wi-Fi and Wi-Fi Direct without User Interaction.	2023-11-07	7.5	CVE-2023-42530
samsung -- android	Improper Certificate Validation in FotaAgent prior to SMR Nov-2023 Release1 allows remote attacker to intercept the network traffic including Firmware information.	2023-11-07	7.5	CVE-2023-42532
samsung -- bixby_voice	Improper verification of intent by broadcast receiver vulnerability in Bixby Voice prior to version 3.3.35.12 allows attackers to access arbitrary data with Bixby Voice privilege.	2023-11-07	7.5	CVE-2023-42543
samsung -- exynos_9810_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem (Exynos 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Modem 5123, Modem 5300, and Auto T5123). Improper handling of a length parameter inconsistency can cause abnormal termination of a mobile phone. This occurs in the RLC task and RLC module.	2023-11-08	7.5	CVE-2023-41111
samsung -- exynos_9810_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem (Exynos 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Modem 5123, Modem 5300, and Auto T5123). A buffer copy, without checking the size of the input, can cause abnormal termination of a mobile phone. This occurs in the RLC task and RLC module.	2023-11-08	7.5	CVE-2023-41112
samsung -- phone	Use of implicit intent for sensitive communication vulnerability in Phone prior to versions 12.7.20.12 in Android 11, 13.1.48, 13.5.28 in Android 12, and 14.7.38 in Android 13 allows attackers to access location data.	2023-11-07	7.5	CVE-2023-42545
schedmd -- slurm	SchedMD Slurm 23.02.x before 23.02.6 and 22.05.x before 22.05.10 allows filesystem race conditions for gaining ownership of a file, overwriting a file, or deleting files.	2023-11-03	7	CVE-2023-41914 MISC CONFIRM
softing -- smartlink_sw-ht	Weak ciphers in Softing smartLink SW-HT before 1.30 are enabled during secure communication (SSL).	2023-11-06	7.5	CVE-2022-48193 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
squid-cache -- squid	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a NULL pointer dereference bug Squid is vulnerable to a Denial of Service attack against Squid's Gopher gateway. The gopher protocol is always available and enabled in Squid prior to Squid 6.0.1. Responses triggering this bug are possible to be received from any gopher server, even those without malicious intent. Gopher support has been removed in Squid version 6.0.1. Users are advised to upgrade. Users unable to upgrade should reject all gopher URL requests.	2023-11-06	7.5	CVE-2023-46728 MISC MISC
squid-cache -- squid	Squid is vulnerable to a Denial of Service, where a remote attacker can perform buffer overflow attack by writing up to 2 MB of arbitrary data to heap memory when Squid is configured to accept HTTP Digest Authentication.	2023-11-03	7.5	CVE-2023-46847 MISC MISC MISC MISC MISC MISC
squid-cache -- squid	Squid is vulnerable to Denial of Service, where a remote attacker can perform DoS by sending ftp:// URLs in HTTP Request messages or constructing ftp:// URLs from FTP Native input.	2023-11-03	7.5	CVE-2023-46848 MISC MISC MISC MISC MISC
squid-cache -- squid	Squid is vulnerable to Denial of Service attack against HTTP and HTTPS clients due to an Improper Handling of Structural Elements bug.	2023-11-03	7.5	CVE-2023-5824 MISC MISC MISC
squidex.io -- squidex	Squidex is an open source headless CMS and content management hub. Affected versions are subject to an arbitrary file write vulnerability in the backup restore feature which allows an authenticated attacker to gain remote code execution (RCE). Squidex allows users with the `squidex.admin.restore` permission to create and restore backups. Part of these backups are the assets uploaded to an App. For each asset, the backup zip archive contains a `.asset` file with the actual content of the asset as well as a related `AssetCreatedEventV2` event, which is stored in a JSON file. Amongst other things, the JSON file contains the event type (`AssetCreatedEventV2`), the ID of the asset (`46c05041-9588-4179-b5eb-ddfcd9463e1e`), its filename (`test.txt`), and its file version (`0`). When a backup with this event is restored, the `BackupAssets.ReadAssetAsync` method is responsible for re-creating the asset. For this purpose, it determines the name of the `.asset` file in the zip archive, reads its content, and stores the content in the filestore. When the asset is stored in the filestore via the UploadAsync method, the assetId and fileVersion are passed as arguments. These are further passed to the method GetFileName, which determines the filename where the asset should be stored. The	2023-11-07	7.2	CVE-2023-46253

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assetId is inserted into the filename without any sanitization and an attacker with squidex.admin.restore privileges to run arbitrary operating system commands on the underlying server (RCE).			
strapi -- strapi	strapi is an open-source headless CMS. Versions prior to 4.13.1 did not properly restrict write access to fielded marked as private in the user registration endpoint. As such malicious users may be able to errantly modify their user records. This issue has been addressed in version 4.13.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-11-06	7.5	CVE-2023-39345 MISC
swtpm -- swtpm	In swtpm before 0.4.2 and 0.5.x before 0.5.1, a local attacker may be able to overwrite arbitrary files via a symlink attack against a temporary file such as TMP2-00.permall.	2023-11-03	7.1	CVE-2020-28407 MISC CONFIRM CONFIRM
sysaid -- sysaid_on-premises	In SysAid On-Premise before 23.3.36, a path traversal vulnerability leads to code execution after an attacker writes a file to the Tomcat webroot, as exploited in the wild in November 2023.	2023-11-10	9.8	CVE-2023-47246
wordpress -- wordpress	The Templately WordPress plugin before 2.2.6 does not properly authorize the `saved-templates/delete` REST API call, allowing unauthenticated users to delete arbitrary posts.	2023-11-06	7.5	CVE-2023-5454 MISC
tenda -- ax1806_firmware	Tenda AX1806 V1.0.0.1 contains a heap overflow vulnerability in setSchedWifi function, in which the src and v12 are directly obtained from http request parameter schedStartTime and schedEndTime without checking their size.	2023-11-07	9.1	CVE-2023-47455
tenda -- ax1806_firmware	Tenda AX1806 V1.0.0.1 contains a stack overflow vulnerability in function sub_455D4, called by function fromSetWirelessRepeat.	2023-11-07	9.1	CVE-2023-47456
tigera -- calico_cloud	In certain conditions for Calico Typha (v3.26.2, v3.25.1 and below), and Calico Enterprise Typha (v3.17.1, v3.16.3, v3.15.3 and below), a client TLS handshake can block the Calico Typha server indefinitely, resulting in denial of service. The TLS Handshake() call is performed inside the main server handle for loop without any timeout allowing an unclean TLS handshake to block the main loop indefinitely while other connections will be idle waiting for that handshake to finish.	2023-11-06	7.5	CVE-2023-41378 MISC MISC MISC
tyk -- tyk	Blind SQL injection in api_id parameter in Tyk Gateway version 5.0.3 allows attacker to access and dump the database via a crafted SQL query.	2023-11-07	9.8	CVE-2023-42283
tyk -- tyk	Blind SQL injection in api_version parameter in Tyk Gateway version 5.0.3 allows attacker to access and dump the database via a crafted SQL query.	2023-11-07	9.8	CVE-2023-42284
utoronto -- pcrs	PCRS <= 3.11 (d0de1e) "Questions" page and "Code editor" page are vulnerable to remote code execution (RCE) by escaping Python sandboxing.	2023-11-03	9.9	CVE-2023-46404 MISC MISC
vaerys-dawn -- discordsailv2	A vulnerability was found in Vaerys-Dawn DiscordSailv2 up to 2.10.2. It has been declared	2023-11-05	9.8	CVE-2018-25092

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	as critical. Affected by this vulnerability is an unknown functionality of the component Command Mention Handler. The manipulation leads to improper access controls. Upgrading to version 2.10.3 is able to address this issue. The patch is named cc12e0be82a5d05d9f359ed8e56088 f4f8b8eb69. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-244483.			MISC MISC MISC MISC
vaerys-dawn -- discordsailv2	A vulnerability was found in Vaerys-Dawn DiscordSailv2 up to 2.10.2. It has been rated as critical. Affected by this issue is some unknown functionality of the component Tag Handler. The manipulation leads to improper access controls. Upgrading to version 2.10.3 is able to address this issue. The name of the patch is cc12e0be82a5d05d9f359ed8e56088f4f8b8eb69. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-244484.	2023-11-06	9.8	CVE-2018-25093 MISC MISC MISC MISC
veeam -- one	A vulnerability in Veeam ONE allows an unauthenticated user to gain information about the SQL server connection Veeam ONE uses to access its configuration database. This may lead to remote code execution on the SQL server hosting the Veeam ONE configuration database.	2023-11-07	9.8	CVE-2023-38547
videolan -- vlc_media_player	Videolan VLC prior to version 3.0.20 contains an incorrect offset read that leads to a Heap-Based Buffer Overflow in function GetPacket() and results in a memory corruption.	2023-11-07	9.8	CVE-2023-47359
videolan -- vlc_media_player	Videolan VLC prior to version 3.0.20 contains an Integer underflow that leads to an incorrect packet length.	2023-11-07	7.5	CVE-2023-47360
webidsupport -- webid	WeBid <=1.2.2 is vulnerable to code injection via admin/categoriestrans.php.	2023-11-08	9.8	CVE-2023-47397
weintek -- easybuilder_pro	Weintek EasyBuilder Pro contains a vulnerability that, even when the private key is immediately deleted after the crash report transmission is finished, the private key is exposed to the public, which could result in obtaining remote control of the crash report server.	2023-11-06	9.8	CVE-2023-5777 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Lenderd 1003 Mortgage Application.This issue affects 1003 Mortgage Application: from n/a through 1.75.	2023-11-07	9.8	CVE-2022-45357
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Scott Reilly Commenter Emails.This issue affects Commenter Emails: from n/a through 2.6.1.	2023-11-07	9.8	CVE-2022-45360
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in WebToffee WordPress Comments Import & Export.This issue affects WordPress Comments Import & Export: from n/a through 2.3.1.	2023-11-07	9.8	CVE-2022-45370
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jason Crouse, VeronaLabs Slimstat Analytics	2023-11-06	9.8	CVE-2022-45373 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows SQL Injection.This issue affects Slimstat Analytics: from n/a through 5.0.4.			
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Paytm Paytm Payment Gateway paytm-payments allows SQL Injection.This issue affects Paytm Payment Gateway: from n/a through 2.7.3.	2023-11-03	9.8	CVE-2022-45805 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Icegram Icegram Express - Email Marketing, Newsletters and Automation for WordPress & WooCommerce.This issue affects Icegram Express - Email Marketing, Newsletters and Automation for WordPress & WooCommerce: from n/a through 5.5.2.	2023-11-07	9.8	CVE-2022-45810
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Paul Ryley Site Reviews. This issue affects Site Reviews: from n/a through 6.2.0.	2023-11-07	9.8	CVE-2022-46801
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in WebToffee Product Reviews Import Export for WooCommerce. This issue affects Product Reviews Import Export for WooCommerce: from n/a through 1.4.8.	2023-11-07	9.8	CVE-2022-46802
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Noptin Newsletter Simple Newsletter Plugin - Noptin. This issue affects Simple Newsletter Plugin - Noptin: from n/a through 1.9.5.	2023-11-07	9.8	CVE-2022-46803
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Repute Infosystems ARMember armember-membership allows SQL Injection.This issue affects ARMember: from n/a through 3.4.11.	2023-11-03	9.8	CVE-2022-46808 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in WPDeveloper ReviewX - Multi-criteria Rating & Reviews for WooCommerce.This issue affects ReviewX - Multi-criteria Rating & Reviews for WooCommerce: from n/a through 1.6.7.	2023-11-07	9.8	CVE-2022-46809
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Gopi Ramasamy Email posts to subscribers allows SQL Injection.This issue affects Email posts to subscribers: from n/a through 6.2.	2023-11-03	9.8	CVE-2022-46818 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Weblizar Coming Soon Page - Responsive Coming Soon & Maintenance Mode allows SQL Injection.This issue affects Coming Soon Page - Responsive Coming Soon & Maintenance Mode: from n/a through 1.5.9.	2023-11-06	9.8	CVE-2022-46849 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spiffy Plugins Spiffy Calendar spiffy-calendar allows SQL Injection.This issue affects Spiffy Calendar: from n/a through 4.9.1.	2023-11-03	9.8	CVE-2022-46859 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	2023-11-06	9.8	CVE-2022-46860

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in KaizenCoders Short URL allows SQL Injection.This issue affects Short URL: from n/a through 1.6.4.			MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Online ADA Accessibility Suite by Online ADA allows SQL Injection.This issue affects Accessibility Suite by Online ADA: from n/a through 4.11.	2023-11-06	9.8	CVE-2022-47420 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Neshan Maps Platform Neshan Maps neshan-maps allows SQL Injection.This issue affects Neshan Maps: from n/a through 1.1.4.	2023-11-03	9.8	CVE-2022-47426 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WpDevArt Booking calendar, Appointment Booking System allows SQL Injection.This issue affects Booking calendar, Appointment Booking System: from n/a through 3.2.7.	2023-11-06	9.8	CVE-2022-47428 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Weblizar The School Management - Education & Learning Management allows SQL Injection.This issue affects The School Management - Education & Learning Management: from n/a through 4.1.	2023-11-06	9.8	CVE-2022-47430 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Kemal YAZICI - PluginPress Shortcode IMDB allows SQL Injection.This issue affects Shortcode IMDB: from n/a through 6.0.8.	2023-11-06	9.8	CVE-2022-47432 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Web-X Be POPIA Compliant be-popia-compliant allows SQL Injection.This issue affects Be POPIA Compliant: from n/a through 1.2.0.	2023-11-03	9.8	CVE-2022-47445 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tips and Tricks HQ, Peter Petreski Simple Photo Gallery simple-photo-gallery allows SQL Injection.This issue affects Simple Photo Gallery: from n/a through v1.8.1.	2023-11-03	9.8	CVE-2022-47588 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in GiveWP.This issue affects GiveWP: from n/a through 2.25.1.	2023-11-07	9.8	CVE-2023-22719
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Muneeb Form Builder | Create Responsive Contact Forms. This issue affects Form Builder | Create Responsive Contact Forms: from n/a through 1.9.9.0.	2023-11-07	9.8	CVE-2023-23796
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection.This issue affects Tutor LMS: from n/a through 2.1.10.	2023-11-03	9.8	CVE-2023-25700 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zendrop Zendrop - Global Dropshipping zendrop-dropshipping-and-fulfillment allows SQL	2023-11-03	9.8	CVE-2023-25960 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Injection.This issue affects Zendrop - Global Dropshipping: from n/a through 1.0.0.			
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Chris Richardson MapPress Maps for WordPress mappress-google-maps-for-wordpress allows SQL Injection. This issue affects MapPress Maps for WordPress: from n/a through 2.85.4.	2023-11-03	9.8	CVE-2023-26015 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sajjad Hossain WP Reroute Email allows SQL Injection.This issue affects WP Reroute Email: from n/a through 1.4.6.	2023-11-06	9.8	CVE-2023-27605 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in biztechc Copy or Move Comments allows SQL Injection.This issue affects Copy or Move Comments: from n/a through 5.0.4.	2023-11-06	9.8	CVE-2023-28748 MISC
wordpress -- wordpress	The MStore API plugin for WordPress is vulnerable to Unauthorized Account Access and Privilege Escalation in versions up to, and including, 4.10.7 due to improper implementation of the Apple login feature. This allows unauthenticated attackers to log in as any user as long as they know the user's email address. We are disclosing this issue as the developer has not yet released a patch, but continues to release updates and we escalated this issue to the plugin's team 30 days ago.	2023-11-03	9.8	CVE-2023-3277 MISC MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP Project Manager wedevs-project-manager allows SQL Injection.This issue affects WP Project Manager: from n/a through 2.6.0.	2023-11-03	9.8	CVE-2023-34383 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Creative Solutions Contact Form Generator : Creative form builder for WordPress allows SQL Injection.This issue affects Contact Form Generator : Creative form builder for WordPress: from n/a through 2.6.0.	2023-11-06	9.8	CVE-2023-35911 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Favethemes Houzez - Real Estate WordPress Theme allows SQL Injection.This issue affects Houzez - Real Estate WordPress Theme: from n/a through 1.3.4.	2023-11-03	9.8	CVE-2023-36529 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Daniel Söderström / Sidney van de Stouwe Subscribe to Category allows SQL Injection.This issue affects Subscribe to Category: from n/a through 2.7.4.	2023-11-06	9.8	CVE-2023-38382 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RedNao Donations Made Easy - Smart Donations allows SQL Injection.This issue affects Donations Made Easy - Smart Donations: from n/a through 4.0.12.	2023-11-06	9.8	CVE-2023-40207 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aiyaz, maheshpatel Contact form 7 Custom validation allows SQL Injection.This issue affects Contact form 7 Custom validation: from n/a through 1.1.3.	2023-11-06	9.8	CVE-2023-40609 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David F. Carr RSVPMaker rsvpmaker allows SQL Injection.This issue affects RSVPMaker: from n/a through 10.6.6.	2023-11-03	9.8	CVE-2023-41652 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ilGhera Woocommerce Support System allows SQL Injection.This issue affects Woocommerce Support System: from n/a through 1.2.1.	2023-11-06	9.8	CVE-2023-41685 MISC
wordpress -- wordpress	Bon Presta boninstagramcarousel between v5.2.1 to v7.0.0 was discovered to contain a Server-Side Request Forgery (SSRF) via the url parameter at insta_parser.php. This vulnerability allows attackers to use the vulnerable website as proxy to attack other websites or exfiltrate data via a HTTP call.	2023-11-03	9.8	CVE-2023-43982 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Castos Seriously Simple Stats allows SQL Injection.This issue affects Seriously Simple Stats: from n/a through 1.5.0.	2023-11-06	9.8	CVE-2023-45001 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pressference Pressference Exporter allows SQL Injection.This issue affects Pressference Exporter: from n/a through 1.0.3.	2023-11-06	9.8	CVE-2023-45046 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in InspireUI MStore API allows SQL Injection.This issue affects MStore API: from n/a through 4.0.6.	2023-11-06	9.8	CVE-2023-45055 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Video Gallery by Total-Soft Video Gallery - Best WordPress YouTube Gallery Plugin allows SQL Injection.This issue affects Video Gallery - Best WordPress YouTube Gallery Plugin: from n/a through 2.1.3.	2023-11-06	9.8	CVE-2023-45069 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Page Visit Counter Advanced Page Visit Counter - Most Wanted Analytics Plugin for WordPress allows SQL Injection.This issue affects Advanced Page Visit Counter - Most Wanted Analytics Plugin for WordPress: from n/a through 7.1.1.	2023-11-06	9.8	CVE-2023-45074 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in POSIMYTH Nexter allows SQL Injection.This issue affects Nexter: from n/a through 2.0.3.	2023-11-06	9.8	CVE-2023-45657 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	2023-11-06	9.8	CVE-2023-45830

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in Online ADA Accessibility Suite by Online ADA allows SQL Injection.This issue affects Accessibility Suite by Online ADA: from n/a through 4.11.			MISC
wordpress -- wordpress	The WooCommerce Ninja Forms Product Add-ons WordPress plugin before 1.7.1 does not validate the file to be uploaded, allowing any unauthenticated users to upload arbitrary files to the server, leading to RCE.	2023-11-06	9.8	CVE-2023-5601 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Nakashima Masahiro WP CSV Exporter. This issue affects WP CSV Exporter: from n/a through 2.0.	2023-11-07	8.8	CVE-2022-38702
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Kaushik Kalathiya Export Users Data CSV. This issue affects Export Users Data CSV: from n/a through 2.1.	2023-11-07	8.8	CVE-2022-41616
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Shambix Simple CSV/XLS Exporter. This issue affects Simple CSV/XLS Exporter: from n/a through 1.5.8.	2023-11-07	8.8	CVE-2022-42882
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Patrick Robrecht Posts and Users Stats. This issue affects Posts and Users Stats: from n/a through 1.1.3.	2023-11-07	8.8	CVE-2022-44738
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in anmari amr users. This issue affects amr users: from n/a through 4.59.4.	2023-11-07	8.8	CVE-2022-45348
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Pär Thernström Simple History - user activity log, audit tool. This issue affects Simple History - user activity log, audit tool: from n/a through 3.3.1.	2023-11-07	8.8	CVE-2022-45350
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Narola Infotech Solutions LLP Export Users Data Distinct. This issue affects Export Users Data Distinct: from n/a through 1.3.	2023-11-07	8.8	CVE-2022-46804
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in wpexpertsio Email Templates Customizer and Designer for WordPress and WooCommerce email-templates allows Cross Site Request Forgery.This issue affects Email Templates Customizer and Designer for WordPress and WooCommerce: from n/a through 1.4.2.	2023-11-07	8.8	CVE-2022-47181
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in AyeCode Ltd UsersWP.This issue affects UsersWP: from n/a through 1.2.3.9.	2023-11-07	8.8	CVE-2022-47442
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection.This issue affects Tutor LMS: from n/a through 2.2.0.	2023-11-03	8.8	CVE-2023-25800 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Frédéric Sheedy Etsy Shop plugin <= 3.0.3 versions.	2023-11-09	8.8	CVE-2023-25975
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in WPOmnia KB	2023-11-07	8.8	CVE-2023-25983

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Support.This issue affects KB Support: from n/a through 1.5.84.			
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection.This issue affects Tutor LMS: from n/a through 2.1.10.	2023-11-03	8.8	CVE-2023-25990 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Alex Benfica Publish to Schedule plugin <= 4.4.2 versions.	2023-11-09	8.8	CVE-2023-25994
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Robert Schulz (sprd.Net AG) Spreadshop plugin <= 1.6.5 versions.	2023-11-10	8.8	CVE-2023-29426
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in SuPlugins Superb Social Media Share Buttons and Follow Buttons for WordPress plugin <= 1.1.3 versions.	2023-11-10	8.8	CVE-2023-29428
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in PressTigers Simple Job Board plugin <= 2.10.3 versions.	2023-11-10	8.8	CVE-2023-29440
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Tribulant Newsletters plugin <= 4.8.8 versions.	2023-11-10	8.8	CVE-2023-30478
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Marco Steinbrecher WP BrowserUpdate plugin <= 4.4.1 versions.	2023-11-10	8.8	CVE-2023-31078
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Igor Benic Simple Giveaways - Grow your business, email lists and traffic with contests plugin <= 2.46.0 versions.	2023-11-09	8.8	CVE-2023-31086
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in JoomSky JS Job Manager plugin <= 2.0.0 versions.	2023-11-09	8.8	CVE-2023-31087
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Faraz Quazi Floating Action Button plugin <= 1.2.1 versions.	2023-11-09	8.8	CVE-2023-31088
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Chronosly Chronosly Events Calendar plugin <= 2.6.2 versions.	2023-11-09	8.8	CVE-2023-31093
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Roland Barker, xnau webdesign Participants Database plugin <= 2.4.9 versions.	2023-11-09	8.8	CVE-2023-31235
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in PeepSo Community by PeepSo - Social Network, Membership, Registration, User Profiles plugin <= 6.0.9.0 versions.	2023-11-09	8.8	CVE-2023-32092
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Criss Swaim TPG Redirect plugin <= 1.0.7 versions.	2023-11-09	8.8	CVE-2023-32093
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Daniel Powney Multi Rating plugin <= 5.0.6 versions.	2023-11-09	8.8	CVE-2023-32125
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in xtemos WoodMart - Multipurpose WooCommerce Theme <= 7.1.1 versions.	2023-11-09	8.8	CVE-2023-32500
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in E4J s.R.L. VikBooking Hotel Booking Engine & PMS plugin <= 1.6.1 versions.	2023-11-09	8.8	CVE-2023-32501

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Sybre Waaijer Pro Mime Types - Manage file media types plugin <= 1.0.7 versions.	2023-11-09	8.8	CVE-2023-32502
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in ShortPixel ShortPixel Adaptive Images - WebP, AVIF, CDN, Image Optimization plugin <= 3.7.1 versions.	2023-11-09	8.8	CVE-2023-32512
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Designs & Code Forget About Shortcode Buttons plugin <= 2.1.2 versions.	2023-11-09	8.8	CVE-2023-32579
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WP Reactions, LLC WP Reactions Lite plugin <= 1.3.8 versions.	2023-11-09	8.8	CVE-2023-32587
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Palasthotel by Edward Bock, Katharina Rompf Sunny Search plugin <= 1.0.2 versions.	2023-11-09	8.8	CVE-2023-32592
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Benedict B., Maciej Gryniuk Hyphenator plugin <= 5.1.5 versions.	2023-11-09	8.8	CVE-2023-32594
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in LOKALYZE CALL ME NOW plugin <= 3.0 versions.	2023-11-09	8.8	CVE-2023-32602
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Web_Trendy WP Custom Cursors | WordPress Cursor Plugin plugin < 3.2 versions.	2023-11-09	8.8	CVE-2023-32739
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce Product Recommendations plugin <= 2.3.0 versions.	2023-11-09	8.8	CVE-2023-32744
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce AutomateWoo plugin <= 5.7.1 versions.	2023-11-09	8.8	CVE-2023-32745
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce Product Add-Ons plugin <= 6.1.3 versions.	2023-11-09	8.8	CVE-2023-32794
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WP Inventory Manager plugin <= 2.1.0.13 versions.	2023-11-09	8.8	CVE-2023-34002
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Guillemant David WP Full Auto Tags Manager plugin <= 2.2 versions.	2023-11-09	8.8	CVE-2023-34024
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in LWS LWS Hide Login plugin <= 2.1.6 versions.	2023-11-09	8.8	CVE-2023-34025
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Pascal Casier bbPress Toolkit plugin <= 1.0.12 versions.	2023-11-09	8.8	CVE-2023-34031
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Malinky Ajax Pagination and Infinite Scroll plugin <= 2.0.1 versions.	2023-11-09	8.8	CVE-2023-34033
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in SAKURA Internet Inc. TS Webfonts for ??????????? plugin <= 3.1.2 versions.	2023-11-09	8.8	CVE-2023-34169
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Kenth Hagström WP-Cache.Com plugin <= 1.1.1 versions.	2023-11-09	8.8	CVE-2023-34177

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Groundhogg Inc. Groundhogg plugin <= 2.7.11 versions.	2023-11-09	8.8	CVE-2023-34178
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WP-Cirrus plugin <= 0.6.11 versions.	2023-11-09	8.8	CVE-2023-34181
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Peter Shaw LH Password Changer plugin <= 1.55 versions.	2023-11-09	8.8	CVE-2023-34182
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Didier Sampaolo SpamReferrerBlock plugin <= 2.22 versions.	2023-11-09	8.8	CVE-2023-34371
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WPClever WPC Smart Wishlist for WooCommerce plugin <= 4.7.1 versions.	2023-11-09	8.8	CVE-2023-34386
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nucleus_genius Quasar form free - Contact Form Builder for WordPress allows SQL Injection.This issue affects Quasar form free - Contact Form Builder for WordPress: from n/a through 6.0.	2023-11-04	8.8	CVE-2023-35910 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in BestWebSoft Post to CSV by BestWebSoft.This issue affects Post to CSV by BestWebSoft: from n/a through 1.4.0.	2023-11-07	8.8	CVE-2023-36527
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Smartypants SP Project & Document Manager allows SQL Injection.This issue affects SP Project & Document Manager: from n/a through 4.67.	2023-11-03	8.8	CVE-2023-36677 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in wpWax Directorist - WordPress Business Directory Plugin with Classified Ads Listing.This issue affects Directorist - WordPress Business Directory Plugin with Classified Ads Listings: from n/a through 7.7.1.	2023-11-07	8.8	CVE-2023-41798
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in bPlugins LLC Icons Font Loader allows SQL Injection. This issue affects Icons Font Loader: from n/a through 1.1.2.	2023-11-06	8.8	CVE-2023-46084 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Mat Bao Corp WP Helper Premium plugin <= 4.5.1 versions.	2023-11-09	8.8	CVE-2023-46614
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Djo Original texts Yandex WebMaster plugin <= 1.18 versions.	2023-11-06	8.8	CVE-2023-46775 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Serena Villa Auto Excerpt everywhere plugin <= 1.5 versions.	2023-11-06	8.8	CVE-2023-46776 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Custom Login Page | Temporary Users | Rebrand Login | Login Captcha plugin <= 1.1.3 versions.	2023-11-06	8.8	CVE-2023-46777 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in TheFreeWindows Auto Limit Posts Reloaded plugin <= 2.5 versions.	2023-11-06	8.8	CVE-2023-46778 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in EasyRecipe plugin <= 3.5.3251 versions.	2023-11-06	8.8	CVE-2023-46779 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Alter plugin <= 1.0 versions.	2023-11-06	8.8	CVE-2023-46780 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Roland Murg Current Menu Item for Custom Post Types plugin <= 1.5 versions.	2023-11-06	8.8	CVE-2023-46781 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) leading to a Stored Cross-Site Scripting (XSS) vulnerability in Nazmul Hossain Nihal Login Screen Manager plugin <= 3.5.2 versions.	2023-11-06	8.8	CVE-2023-47182 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Kadence WP Kadence WooCommerce Email Designer plugin <= 1.5.11 versions.	2023-11-06	8.8	CVE-2023-47186 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WebberZone Top 10 - WordPress Popular posts by WebberZone plugin <= 3.3.2 versions.	2023-11-09	8.8	CVE-2023-47238
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in ThemeKraft TK Google Fonts GDPR Compliant plugin <= 2.2.11 versions.	2023-11-06	8.8	CVE-2023-5823 MISC
wordpress -- wordpress	The Awesome Support WordPress plugin before 6.1.5 does not sanitize file paths when deleting temporary attachment files, allowing a ticket submitter to delete arbitrary files on the server.	2023-11-06	8.1	CVE-2023-5355 MISC
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in Solwin Infotech User Blocker. This issue affects User Blocker: from n/a through 1.5.5.	2023-11-07	7.2	CVE-2022-45078
wordpress -- wordpress	Improper Neutralization of Formula Elements in a CSV File vulnerability in WPEkaClub WP Cookie Consent (for GDPR, CCPA & ePrivacy).This issue affects WP Cookie Consent (for GDPR, CCPA & ePrivacy): from n/a through 2.2.5.	2023-11-07	7.2	CVE-2023-23678
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Highfivery LLC Zero Spam for WordPress allows SQL Injection.This issue affects Zero Spam for WordPress: from n/a through 5.4.4.	2023-11-03	7.2	CVE-2023-32121 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rolf van Gelder Order Your Posts Manually allows SQL Injection.This issue affects Order Your Posts Manually: from n/a through 2.2.5.	2023-11-03	7.2	CVE-2023-32508 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in IT Path Solutions PVT LTD Contact Form to Any API allows SQL Injection.This issue affects Contact Form to Any API: from n/a through 1.1.2.	2023-11-04	7.2	CVE-2023-32741 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Groundhogg Inc. Groundhogg allows SQL Injection.This issue affects Groundhogg: from n/a through 2.7.11.	2023-11-03	7.2	CVE-2023-34179 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	2023-11-04	7.2	CVE-2023-38391

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in Themesgrove Onepage Builder allows SQL Injection.This issue affects Onepage Builder: from n/a through 2.4.1.			MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Demonisblack demon image annotation allows SQL Injection.This issue affects demon image annotation: from n/a through 5.1.	2023-11-04	7.2	CVE-2023-40215 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Milan Petrovic GD Security Headers allows auth. (admin+) SQL Injection.This issue affects GD Security Headers: from n/a through 1.7.	2023-11-06	7.2	CVE-2023-46821 MISC
wordpress -- wordpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Avirtum ImageLinks Interactive Image Builder for WordPress allows SQL Injection.This issue affects ImageLinks Interactive Image Builder for WordPress: from n/a through 1.5.4.	2023-11-06	7.2	CVE-2023-46823 MISC
wordpress -- wordpress	The History Log by click5 WordPress plugin before 1.0.13 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by admin users when using the Smash Balloon Social Photo Feed plugin alongside it.	2023-11-06	7.2	CVE-2023-5082 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Martin Gibson Auto Publish for Google My Business plugin <= 3.7 versions.	2023-11-09	8.8	CVE-2023-47237
wpn-xm -- wpn-xm	A local file inclusion vulnerability has been found in WPN-XM Serverstack affecting version 0.8.6, which would allow an unauthenticated user to perform a local file inclusion (LFI) via the /tools/webinterface/index.php?page parameter by sending a GET request. This vulnerability could lead to the loading of a PHP file on the server, leading to a critical webshell exploit.	2023-11-03	9.8	CVE-2023-4591 MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki doesn't properly escape the section URL parameter that is used in the code for displaying administration sections. This allows any user with read access to the document \`XWiki.AdminSheet\` (by default, everyone including unauthenticated users) to execute code including Groovy code. This impacts the confidentiality, integrity and availability of the whole XWiki instance. This vulnerability has been patched in XWiki 14.10.14, 15.6 RC1 and 15.5.1. Users are advised to upgrade. Users unablr to upgrade may apply the fix in commit \`fec8e0e53f9\` manually. Alternatively, to protect against attacks from unauthenticated users, view right for guests can be removed from this document (it is only needed for space and wiki admins).	2023-11-06	9.8	CVE-2023-46731 MISC MISC MISC MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to execute a content with the right of any user via a crafted URL. A user must have \`programming\` privileges	2023-11-07	8.8	CVE-2023-46242

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in order to exploit this vulnerability. This issue has been patched in XWiki 14.10.7 and 15.2RC1. Users are advised to upgrade. There are no known workarounds for for this vulnerability.			
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible for a user to execute any content with the right of an existing document's content author, provided the user have edit right on it. A crafted URL of the form ` /xwiki/bin/edit//?content=%7B%7Bgroovy%7D%7Dprintln%28%22Hello+from+Groovy%21%22%29%7B%7B%2Fgroovy%7D%7D&xpage=view` can be used to execute arbitrary groovy code on the server. This vulnerability has been patched in XWiki versions 14.10.6 and 15.2RC1. Users are advised to update. There are no known workarounds for this issue.	2023-11-07	8.8	CVE-2023-46243
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible for a user to write a script in which any velocity content is executed with the right of any other document content author. Since this API require programming right and the user does not have it, the expected result is `$doc.document.authors.contentAuthor` (not executed script), unfortunately with the security vulnerability it is possible for the attacker to get `XWiki.superadmin` which shows that the title was executed with the right of the unmodified document. This has been patched in XWiki versions 14.10.7 and 15.2RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-11-07	8.8	CVE-2023-46244
xxyopen -- novel-plus	SQL injection vulnerability in Novel-Plus v.4.2.0 allows a remote attacker to execute arbitrary code via a crafted script to the sort parameter in /common/log/list.	2023-11-05	9.8	CVE-2023-46981 MISC
zavio -- cf7500_firmware	Zavio CF7500, CF7300, CF7201, CF7501, CB3211, CB3212, CB5220, CB6231, B8520, B8220, and CD321 IP Cameras with firmware version M2.1.6.05 are vulnerable to stack-based overflows. During the process of updating certain settings sent from incoming network requests, the product does not sufficiently check or validate allocated buffer size. This may lead to remote code execution.	2023-11-08	9.8	CVE-2023-39435
zavio -- cf7500_firmware	Zavio CF7500, CF7300, CF7201, CF7501, CB3211, CB3212, CB5220, CB6231, B8520, B8220, and CD321 IP Cameras with firmware version M2.1.6.05 are vulnerable to multiple instances of stack-based overflows. While processing XML elements from incoming network requests, the product does not sufficiently check or validate allocated buffer size. This may lead to remote code execution.	2023-11-08	9.8	CVE-2023-3959
zavio -- cf7500_firmware	Zavio CF7500, CF7300, CF7201, CF7501, CB3211, CB3212, CB5220, CB6231, B8520, B8220, and CD321 IP Cameras with firmware	2023-11-08	9.8	CVE-2023-4249

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version M2.1.6.05 has a command injection vulnerability in their implementation of their binaries and handling of network requests.			
zavio -- cf7500_firmware	Zavio CF7500, CF7300, CF7201, CF7501, CB3211, CB3212, CB5220, CB6231, B8520, B8220, and CD321 IP Cameras with firmware version M2.1.6.05 are vulnerable to multiple instances of stack-based overflows. During the processing and parsing of certain fields in XML elements from incoming network requests, the product does not sufficiently check or validate allocated buffer size. This may lead to remote code execution.	2023-11-08	9.8	CVE-2023-43755
zavio -- cf7500_firmware	Zavio CF7500, CF7300, CF7201, CF7501, CB3211, CB3212, CB5220, CB6231, B8520, B8220, and CD321 IP Cameras with firmware version M2.1.6.05 are vulnerable to multiple instances of stack-based overflows. While parsing certain XML elements from incoming network requests, the product does not sufficiently check or validate allocated buffer size. This may lead to remote code execution.	2023-11-08	9.8	CVE-2023-45225
zohocorp -- manageengine_desktop_central	A SSRF vulnerability has been found in ManageEngine Desktop Central affecting version 9.1.0, specifically the /smtpConfig.do component. This vulnerability could allow an authenticated attacker to launch targeted attacks, such as a cross-port attack, service enumeration and other attacks via HTTP requests.	2023-11-03	8.8	CVE-2023-4769 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- allura	Allura Discussion and Allura Forum importing does not restrict URL values specified in attachments. Project administrators can run these imports, which could cause Allura to read local files and expose them. Exposing internal files then can lead to other exploits, like session hijacking, or remote code execution. This issue affects Apache Allura from 1.0.1 through 1.15.0. Users are recommended to upgrade to version 1.16.0, which fixes the issue. If you are unable to upgrade, set "disable_entry_points.allura.importers = forge-tracker, forge-discussion" in your .ini config file.	2023-11-07	4.9	CVE-2023-46851
apache -- ofbiz	Missing Authentication in Apache Software Foundation Apache OFBiz when using the Solr plugin. This issue affects Apache OFBiz: before 18.12.09. Users are recommended to upgrade to version 18.12.09	2023-11-07	5.3	CVE-2023-46819
arm -- bifrost_gpu_kernel_driver	A local non-privileged user can make GPU processing operations that expose sensitive data from previously freed memory.	2023-11-07	5.5	CVE-2023-4272

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bootboxjs -- bootbox	Cross Site Scripting vulnerability in BootBox Bootbox.js v.3.2 through 6.0 allows a remote attacker to execute arbitrary code via a crafted payload to alert(), confirm(), prompt() functions.	2023-11-07	6.1	CVE-2023-46998
clastix -- capsule	capsule-proxy is a reverse proxy for Capsule kubernetes multi-tenancy framework. A bug in the RoleBinding reflector used by \`capsule-proxy\` gives ServiceAccount tenant owners the right to list Namespaces of other tenants backed by the same owner kind and name. For example, consider two tenants \`solar\` and \`wind\`. Tenant \`solar\`, owned by a ServiceAccount named \`tenant-owner\` in the Namespace \`solar\`. Tenant \`wind\`, owned by a ServiceAccount named \`tenant-owner\` in the Namespace \`wind\`. The Tenant owner \`solar\` would be able to list the namespaces of the Tenant \`wind\` and vice-versa, although this is not correct. The bug introduces an exfiltration vulnerability since allows the listing of Namespace resources of other Tenants, although just in some specific conditions: 1. \`capsule-proxy\` runs with the \`--disable-caching=false\` (default value: \`false\`) and 2. Tenant owners are ServiceAccount, with the same resource name, but in different Namespaces. This vulnerability doesn't allow any privilege escalation on the outer tenant Namespace-scoped resources, since the Kubernetes RBAC is enforcing this. This issue has been addressed in version 0.4.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-11-06	4.3	CVE-2023-46254 MISC MISC
cloudnet360 -- cloudnet360	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in GARY JEZORSKI CloudNet360 plugin <= 3.2.0 versions.	2023-11-08	6.1	CVE-2023-46643
color -- demoiccmax	In International Color Consortium DemoIccMAX 79ecb74, a CIccXmlArrayType:::ParseText function (for unsigned short) in IccUtilXml.cpp in libIccXML.a has an out-of-bounds read.	2023-11-05	6.5	CVE-2023-47249 MISC
cure53 -- dompurify	DOMPurify before 1.0.11 allows reverse tabnabbing in demos/hooks-target-blank-demo.html because links lack a 'rel="noopener noreferrer"' attribute.	2023-11-07	6.1	CVE-2019-25155
docker -- machine	Docker Machine through 0.16.2 allows an attacker, who has control of a worker node, to provide crafted version data, which might potentially trick an administrator into performing an unsafe action (via escape sequence injection), or might have a data size that causes a denial of service to a bastion node. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2023-11-07	6.5	CVE-2023-40453
dstar2018 -- agency	A vulnerability classified as problematic was found in dstar2018 Agency up to 61. Affected by this vulnerability is an unknown functionality of the file search.php. The manipulation of the argument QSType/QuickSearch leads to cross site scripting. The attack can be launched remotely. The patch is named 975b56953efabb434519d9feefcc53685fb8d0ab. It is recommended to apply a patch to	2023-11-07	6.1	CVE-2019-25156

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	fix this issue. The associated identifier of this vulnerability is VDB-244495.			
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.3 before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1. A Regular Expression Denial of Service was possible by adding a large string in timeout input in gitlab-ci.yml file.	2023-11-06	6.5	CVE-2023-3909 MISC MISC
gitlab -- gitlab	An authorization issue affecting GitLab EE affecting all versions from 14.7 prior to 16.3.6, 16.4 prior to 16.4.2, and 16.5 prior to 16.5.1, allowed a user to run jobs in protected environments, bypassing any required approvals.	2023-11-06	6.5	CVE-2023-4700 MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.2 before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1. A low-privileged attacker can point a CI/CD Component to an incorrect path and cause the server to exhaust all available memory through an infinite loop and cause Denial of Service.	2023-11-06	6.5	CVE-2023-5825 MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.0 before 16.3.6, all versions starting from 16.4 before 16.4.2, and all versions starting from 16.5.0 before 16.5.1 which have the `super_sidebar_logged_out` feature flag enabled. Affected versions with this default-disabled feature flag enabled may unintentionally disclose GitLab version metadata to unauthorized actors.	2023-11-06	5.3	CVE-2023-5831 MISC
gitlab -- gitlab	An issue has been discovered in GitLab EE/CE affecting all versions starting before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1 which allows an attacker to block Sidekiq job processor.	2023-11-06	4.3	CVE-2023-3246 MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab EE with Advanced Search affecting all versions from 13.9 to 16.3.6, 16.4 prior to 16.4.2 and 16.5 prior to 16.5.1 that could allow a denial of service in the Advanced Search function by chaining too many syntax operators.	2023-11-06	4.3	CVE-2023-5963 MISC
google -- android	In vdec, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08163896 & ALPS08013430; Issue ID: ALPS07867715.	2023-11-06	6.7	CVE-2023-32818 MISC
google -- android	In secmem, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08161762; Issue ID: ALPS08161762.	2023-11-06	6.7	CVE-2023-32834 MISC
google -- android	In keyinstall, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed	2023-11-06	6.7	CVE-2023-32835 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for exploitation. Patch ID: ALPS08157918; Issue ID: ALPS08157918.			
google -- android	In display, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08126725; Issue ID: ALPS08126725.	2023-11-06	6.7	CVE-2023-32836 MISC
google -- android	In dpe, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310805; Issue ID: ALPS07310805.	2023-11-06	6.7	CVE-2023-32838 MISC
google -- android	In dpe, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262576; Issue ID: ALPS07262576.	2023-11-06	6.7	CVE-2023-32839 MISC
google -- android	In bluethooth service, there is a possible out of bounds reads due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07884130; Issue ID: ALPS07884130.	2023-11-06	5.5	CVE-2023-32825 MISC
gvectors -- wpdiscuz	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in gVectors Team Comments - wpDiscuz plugin <= 7.6.11 versions.	2023-11-06	6.1	CVE-2023-47185 MISC
hillstonenet -- sc-6000-e3960_firmware	Cross Site Scripting (XSS) vulnerability in Hillstone Next Generation FireWall SG-6000-e3960 v.5.5 allows a remote attacker to execute arbitrary code via the use front-end filtering instead of back-end filtering.	2023-11-05	6.1	CVE-2023-46964 MISC
huawei -- emui	Race condition vulnerability in the kernel module. Successful exploitation of this vulnerability may cause variable values to be read with the condition evaluation bypassed.	2023-11-08	5.9	CVE-2022-48613
huawei -- emui	Vulnerability of input parameters being not strictly verified in the input. Successful exploitation of this vulnerability may cause the launcher to restart.	2023-11-08	5.3	CVE-2023-46755
huawei -- emui	Vulnerability of background app permission management in the framework module. Successful exploitation of this vulnerability may cause background apps to start maliciously.	2023-11-08	5.3	CVE-2023-46763
huawei -- emui	Unauthorized startup vulnerability of background apps. Successful exploitation of this vulnerability may cause background apps to start maliciously.	2023-11-08	5.3	CVE-2023-46764
huawei -- harmonyos	Permission control vulnerability in the window management module. Successful exploitation of this vulnerability may cause malicious pop-up windows.	2023-11-08	5.3	CVE-2023-46756
ibm -- content_navigator	IBM Content Navigator 3.0.13 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 259247.	2023-11-03	5.4	CVE-2023-35896 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- robotic_process_automation_for_cloud_pak	A vulnerability in IBM Robotic Process Automation and IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.10, 23.0.0 through 23.0.10 may result in access to client vault credentials. This difficult to exploit vulnerability could allow a low privileged attacker to programmatically access client vault credentials. IBM X-Force ID: 268752.	2023-11-03	6.5	CVE-2023-45189 MISC MISC
ibm -- txseries_for_multiplatforms	IBM CICS TX Standard 11.1, Advanced 10.1, 11.1, and TXSeries for Multiplatforms 8.1, 8.2, 9.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 266059.	2023-11-03	5.4	CVE-2023-42029 MISC MISC MISC
jbig2enc_project -- jbig2enc	jbig2enc v0.28 was discovered to contain a heap-use-after-free via jbig2enc_auto_threshold_using_hash in src/jbig2enc.cc.	2023-11-08	5.5	CVE-2023-46362
jbig2enc_project -- jbig2enc	jbig2enc v0.28 was discovered to contain a SEGV via jbig2_add_page in src/jbig2enc.cc:512.	2023-11-08	5.5	CVE-2023-46363
kaoshifeng -- yunfan_learning_examination_system	An issue in Beijing Yunfan Internet Technology Co., Ltd, Yunfan Learning Examination System v.6.5 allows a remote attacker to obtain sensitive information via the password parameter in the login function.	2023-11-04	5.3	CVE-2023-46963 MISC
kyocera -- d-copia253mf_plus_firmware	Kyocera TASKalfa 4053ci printers through 2VG_S000.002.561 allow identification of valid user accounts via username enumeration because they lead to a "nicht einloggen" error rather than a falsch error.	2023-11-03	5.3	CVE-2023-34261 MISC MISC
kyocera -- d-copia253mf_plus_firmware	Kyocera TASKalfa 4053ci printers through 2VG_S000.002.561 allow /wlmdeu%2f%2e%2e%2f%2e%2e directory traversal to read arbitrary files on the filesystem, even files that require root privileges. NOTE: this issue exists because of an incomplete fix for CVE-2020-23575.	2023-11-03	4.9	CVE-2023-34259 MISC MISC
lenovo -- desktop_bios	A buffer overflow was reported in the BiosExtensionLoader module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43571
lenovo -- desktop_bios	A buffer overflow was reported in the LEMALLDriversConnectedEventHook module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43573
lenovo -- desktop_bios	A buffer overflow was reported in the UltraFunctionTable module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43575
lenovo -- desktop_bios	A buffer overflow was reported in the WMISwSmi module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43576
lenovo -- desktop_bios	A buffer overflow was reported in the ReFlash module in some Lenovo Desktop products that	2023-11-08	6.7	CVE-2023-43577

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may allow a local attacker with elevated privileges to execute arbitrary code.			
lenovo -- desktop_bios	A buffer overflow was reported in the SmiFlash module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43578
lenovo -- desktop_bios	A buffer overflow was reported in the SmuV11Dxe driver in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43579
lenovo -- desktop_bios	A buffer overflow was reported in the SmuV11DxeVMR module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43580
lenovo -- desktop_bios	A buffer overflow was reported in the Update_WMI module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	CVE-2023-43581
lenovo -- desktop_bios	A buffer over-read was reported in the BiosExtensionLoader module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to disclose sensitive information.	2023-11-08	4.4	CVE-2023-43572
lenovo -- desktop_bios	A buffer over-read was reported in the LEMALLDriversConnectedEventHook module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to disclose sensitive information.	2023-11-08	4.4	CVE-2023-43574
linux -- kernel	The brcm80211 component in the Linux kernel through 6.5.10 has a brcmf_cfg80211_detach use-after-free in the device unplugging (disconnect the USB by hotplug) code. For physically proximate attackers with local access, this "could be exploited in a real world scenario." This is related to brcmf_cfg80211_escan_timeout_worker in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c.	2023-11-03	4.3	CVE-2023-47233 MISC MISC
linux -- linux_kernel	A flaw was found in KVM. An improper check in svm_set_x2apic_msr_interception() may allow direct access to host x2apic msrs when the guest resets its apic, potentially leading to a denial of service condition.	2023-11-06	5.5	CVE-2023-5090 MISC MISC
mattermost -- mattermost	Mattermost fails to properly sanitize the request to /api/v4/redirect_location allowing an attacker, sending a specially crafted request to /api/v4/redirect_location, to fill up the memory due to caching large items.	2023-11-06	5.3	CVE-2023-5969 MISC
mattermost -- mattermost	Mattermost fails to properly sanitize the user object when updating the username, resulting in the password hash being included in the response body.	2023-11-06	4.9	CVE-2023-5968 MISC
mattermost -- mattermost	Mattermost fails to properly validate requests to the Calls plugin, allowing an attacker sending a request without a User Agent header to cause a panic and crash the Calls plugin	2023-11-06	4.3	CVE-2023-5967 MISC
mediatek -- lr12a	In modem CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	2023-11-06	6.5	CVE-2023-32840 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution privileges needed. User interaction may be also needed for exploitation Patch ID: MOLY01138425; Issue ID: MOLY01138425 (MSV-862).			
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. There is XSS in youhavenewmessagesmanyusers and youhavenewmessages i18n messages. This is related to MediaWiki: Youhavenewmessagesfromusers.	2023-11-03	5.4	CVE-2023-45360 MISC
mediawiki -- mediawiki	An issue was discovered in DifferenceEngine.php in MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. diff-multi-sameuser (aka "X intermediate revisions by the same user not shown") ignores username suppression. This is an information leak.	2023-11-03	4.3	CVE-2023-45362 MISC
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2023-11-03	6.6	CVE-2023-36022 MISC
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-11-07	6.5	CVE-2023-36409 MISC
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2023-11-03	4.3	CVE-2023-36029 MISC
microsoft -- onenote	Microsoft OneNote Spoofing Vulnerability	2023-11-06	5.4	CVE-2023-36769 MISC
microweber -- microweber	Microweber CMS version 2.0.1 is vulnerable to stored Cross Site Scripting (XSS) via the profile picture file upload functionality.	2023-11-08	5.4	CVE-2023-47379
microweber -- microweber	Improper Access Control in GitHub repository microweber/microweber prior to 2.0.	2023-11-07	4.3	CVE-2023-5976
mitsubishi_electric -- fx5u-32mt/es_firmware	Improper Restriction of Excessive Authentication Attempts vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series CPU modules Web server function allows a remote unauthenticated attacker to prevent legitimate users from logging into the Web server function for a certain period after the attacker has attempted to log in illegally by continuously attempting unauthorized login to the Web server function. The impact of this vulnerability will persist while the attacker continues to attempt unauthorized login.	2023-11-06	5.3	CVE-2023-4625 MISC MISC MISC
moodle -- moodle	The CSV grade import method contained an XSS risk for users importing the spreadsheet, if it contained unsafe content.	2023-11-09	6.1	CVE-2023-5541
moodle -- moodle	The course upload preview contained an XSS risk for users uploading unsafe data.	2023-11-09	6.1	CVE-2023-5547
moodle -- moodle	Wiki comments required additional sanitizing and access restrictions to prevent a stored XSS risk and potential IDOR risk.	2023-11-09	5.4	CVE-2023-5544

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moodle -- moodle	ID numbers displayed in the quiz grading report required additional sanitizing to prevent a stored XSS risk.	2023-11-09	5.4	CVE-2023-5546
msyk -- fmdataapi	A vulnerability classified as problematic has been found in msyk FMDataAPI up to 22. Affected is an unknown function of the file FMDataAPI_Sample.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 23 is able to address this issue. The patch is identified as 3bd1709a8f7b1720529bf5dfc9855ad609f436cf. It is recommended to upgrade the affected component. VDB-244494 is the identifier assigned to this vulnerability.	2023-11-07	6.1	CVE-2021-4431
mybb -- mybb	MyBB is a free and open source forum software. Custom MyCode (BBCode) for the visual editor (_SCEditor_) doesn't escape input properly when rendering HTML, resulting in a DOM-based XSS vulnerability. This weakness can be exploited by pointing a victim to a page where the visual editor is active (e.g. as a post or Private Message) and operates on a maliciously crafted MyCode message. This may occur on pages where message content is pre-filled using a GET/POST parameter, or on reply pages where a previously saved malicious message is quoted. The impact is be mitigated when: 1. the visual editor is disabled globally (_Admin CP ? Configuration ? Settings ? Clickable Smilies and BB Code: [Clickable MyCode Editor](https://github.com/mybb/mybb/blob/mybb_1836/install/resources/settings.xml#L2087-L2094)_ is set to _Off_), or 2. the visual editor is disabled for individual user accounts (_User CP ? Your Profile ? Edit Options_: _Show the MyCode formatting options on the posting pages_ checkbox is not checked). MyBB 1.8.37 resolves this issue with the commit `6dcaf0b4d`. Users are advised to upgrade. Users unable to upgrade may mitigate the impact without upgrading MyBB by changing the following setting (_Admin CP ? Configuration ? Settings_): - _Clickable Smilies and BB Code ? [Clickable MyCode Editor](https://github.com/mybb/mybb/blob/mybb_1836/install/resources/settings.xml#L2087-L2094)_: _Off_. Similarly, individual MyBB forum users are able to disable the visual editor by diabling the account option (_User CP ? Your Profile ? Edit Options_) _Show the MyCode formatting options on the posting pages_.	2023-11-06	6.1	CVE-2023-46251 MISC MISC MISC
mybb -- mybb	Cross Site Scripting vulnerability in Mybb Mybb Forums v.1.8.33 allows a local attacker to execute arbitrary code via the theme Name parameter in the theme management component.	2023-11-06	5.4	CVE-2023-45556 MISC MISC MISC
nasa -- openmct	Cross Site Request Forgery (CSRF) vulnerability in NASA Open MCT (aka openmct) through 3.1.0 allows attackers to view sensitive information via the flexibleLayout plugin.	2023-11-09	6.5	CVE-2023-45884

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nasa -- openmct	Cross Site Scripting (XSS) vulnerability in NASA Open MCT (aka openmct) through 3.1.0 allows attackers to run arbitrary code via the new component feature in the flexibleLayout plugin.	2023-11-09	5.4	CVE-2023-45885
nationaledtech -- boomerang	An issue was discovered in the Boomerang Parental Control application before 13.83 for Android. The app is missing the android:allowBackup="false" attribute in the manifest. This allows the user to back up the internal memory of the app to a PC. This gives the user access to the API token that is used to authenticate requests to the API.	2023-11-03	4.6	CVE-2023-36620 MISC MISC MISC
ni -- topografix_data_plugin	An incorrect permission assignment in the TopoGrafix DataPlugin for GPX could result in information disclosure. An attacker could exploit this vulnerability by getting a user to open a specially crafted data file.	2023-11-08	5.5	CVE-2023-5136
nta -- e-tax	e-Tax software Version3.0.10 and earlier improperly restricts XML external entity references (XXE) due to the configuration of the embedded XML parser. By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	2023-11-06	5.5	CVE-2023-46802 MISC MISC
opensc_project -- opensc	A flaw was found in OpenSC packages that allow a potential PIN bypass. When a token/card is authenticated by one process, it can perform cryptographic operations in other processes when an empty zero-length pin is passed. This issue poses a security risk, particularly for OS logon/screen unlock and for small, permanently connected tokens to computers. Additionally, the token can internally track login status. This flaw allows an attacker to gain unauthorized access, carry out malicious actions, or compromise the system without the user's awareness.	2023-11-06	6.6	CVE-2023-40660 MISC MISC MISC MISC MISC
opensc -- opensc	Several memory vulnerabilities were identified within the OpenSC packages, particularly in the card enrollment process using pkcs15-init when a user or administrator enrolls cards. To take advantage of these flaws, an attacker must have physical access to the computer system and employ a custom-crafted USB device or smart card to manipulate responses to APDUs. This manipulation can potentially allow compromise key generation, certificate loading, and other card management operations during enrollment.	2023-11-06	6.4	CVE-2023-40661 MISC MISC MISC MISC MISC
prestashop -- prestashop	blockreassurance adds an information block aimed at offering helpful information to reassure customers that their store is trustworthy. An ajax function in module blockreassurance allows modifying any value in the configuration table. This vulnerability has been patched in version 5.1.4.	2023-11-09	5.3	CVE-2023-47110
proofpoint -- enterprise_protection	Proofpoint Enterprise Protection contains a stored XSS vulnerability in the AdminUI. An unauthenticated attacker can send a specially crafted email with HTML in the subject which triggers XSS when viewing quarantined messages. This issue affects Proofpoint Enterprise Protection: from 8.20.0 before patch	2023-11-06	6.1	CVE-2023-5771 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	4796, from 8.18.6 before patch 4795 and all other prior versions.			
qnap -- qts	A server-side request forgery (SSRF) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to read application data via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2514 build 20230906 and later QTS 5.1.1.2491 build 20230815 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.1.2488 build 20230812 and later QuTScloud c5.1.0.2498 and later	2023-11-03	4.3	CVE-2023-39301 MISC
qualcomm -- snapdragon	Information Disclosure in WLAN Host when processing WMI event command.	2023-11-07	5.5	CVE-2023-28553
qualcomm -- snapdragon	Information Disclosure in Qualcomm IPC while reading values from shared memory in VM.	2023-11-07	5.5	CVE-2023-28554
qualcomm -- snapdragon	Information disclosure in IOE Firmware while handling WMI command.	2023-11-07	5.5	CVE-2023-28563
qualcomm -- snapdragon	Information disclosure in WLAN HAL while handling the WMI state info command.	2023-11-07	5.5	CVE-2023-28566
qualcomm -- snapdragon	Information disclosure in WLAN HAL when reception status handler is called.	2023-11-07	5.5	CVE-2023-28568
qualcomm -- snapdragon	Information disclosure in WLAN HAL while handling command through WMI interfaces.	2023-11-07	5.5	CVE-2023-28569
ragic -- enterprise_cloud_database	Rogic No-Code Database Builder's file uploading function has insufficient filtering for special characters. A remote attacker with regular user privilege can inject JavaScript to perform XSS (Stored Cross-Site Scripting) attack.	2023-11-03	5.4	CVE-2023-41343 MISC
rapid7 -- velociraptor	Rapid7 Velociraptor versions prior to 0.7.0-4 suffer from a reflected cross site scripting vulnerability. This vulnerability allows attackers to inject JS into the error path, potentially leading to unauthorized execution of scripts within a user's web browser. This vulnerability is fixed in version 0.7.0-04 and a patch is available to download. Patches are also available for version 0.6.9 (0.6.9-1).	2023-11-06	6.1	CVE-2023-5950 MISC
redhat -- 3scale_api_management	A flaw was found In 3Scale Admin Portal. If a user logs out from the personal tokens page and then presses the back button in the browser, the tokens page is rendered from the browser cache.	2023-11-06	5.5	CVE-2023-4910 MISC MISC
redhat -- quay	A flaw was found in Quay. Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. During the pentest, it has been detected that the config-editor page is vulnerable to clickjacking. This flaw allows an attacker to trick an administrator user into clicking on buttons on the config-editor panel, possibly reconfiguring some parts of the Quay instance.	2023-11-07	4.3	CVE-2023-4956
redmine -- redmine	Redmine before 4.2.11 and 5.0.x before 5.0.6 allows XSS in a Markdown formatter.	2023-11-05	6.1	CVE-2023-47258 MISC
redmine -- redmine	Redmine before 4.2.11 and 5.0.x before 5.0.6 allows XSS in the Textile formatter.	2023-11-05	6.1	CVE-2023-47259

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
redmine -- redmine	Redmine before 4.2.11 and 5.0.x before 5.0.6 allows XSS via thumbnails.	2023-11-05	6.1	CVE-2023-47260 MISC
roundcube -- webmail	Roundcube 1.5.x before 1.5.6 and 1.6.x before 1.6.5 allows XSS via a Content-Type or Content-Disposition header (used for attachment preview or download).	2023-11-06	6.1	CVE-2023-47272 MISC MISC MISC
samba -- samba	A vulnerability was discovered in Samba, where the flaw allows SMB clients to truncate files, even with read-only permissions when the Samba VFS module "acl_xattr" is configured with "acl_xattr:ignore system acls = yes". The SMB protocol allows opening files when the client requests read-only access but then implicitly truncates the opened file to 0 bytes if the client specifies a separate OVERWRITE create disposition request. The issue arises in configurations that bypass kernel file system permissions checks, relying solely on Samba's permissions.	2023-11-03	6.5	CVE-2023-4091 MISC MISC MISC MISC MISC MISC
samba -- samba	A design flaw was found in Samba's DirSync control implementation, which exposes passwords and secrets in Active Directory to privileged users and Read-Only Domain Controllers (RODCs). This flaw allows RODCs and users possessing the GET_CHANGES right to access all attributes, including sensitive secrets and passwords. Even in a default setup, RODC DC accounts, which should only replicate some passwords, can gain access to all domain secrets, including the vital krbtgt, effectively eliminating the RODC / DC distinction. Furthermore, the vulnerability fails to account for error conditions (fail open), like out-of-memory situations, potentially granting access to secret attributes, even under low-privileged attacker influence.	2023-11-07	6.5	CVE-2023-4154
samba -- samba	A vulnerability was found in Samba's "rpcecho" development server, a non-Windows RPC server used to test Samba's DCE/RPC stack elements. This vulnerability stems from an RPC function that can be blocked indefinitely. The issue arises because the "rpcecho" service operates with only one worker in the main RPC task, allowing calls to the "rpcecho" server to be blocked for a specified time, causing service disruptions. This disruption is triggered by a "sleep()" call in the "dcesrv_echo_TestSleep()" function under specific conditions. Authenticated users or attackers can exploit this vulnerability to make calls to the "rpcecho" server, requesting it to block for a specified duration, effectively disrupting most services and leading to a complete denial of service on the AD DC. The DoS affects all other services as "rpcecho" runs in the main RPC task.	2023-11-06	6.5	CVE-2023-42669 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samba -- samba	A flaw was found in Samba. It is susceptible to a vulnerability where multiple incompatible RPC listeners can be initiated, causing disruptions in the AD DC service. When Samba's RPC server experiences a high load or unresponsiveness, servers intended for non-AD DC purposes (for example, NT4-emulation "classic DCs") can erroneously start and compete for the same unix domain sockets. This issue leads to partial query responses from the AD DC, causing issues such as "The procedure number is out of range" when using tools like Active Directory Users. This flaw allows an attacker to disrupt AD DC services.	2023-11-03	6.5	CVE-2023-42670 MISC MISC MISC MISC MISC
samsung -- account	Use of implicit intent for sensitive communication vulnerability in startAgreeToDisclaimerActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	CVE-2023-42546
samsung -- account	Use of implicit intent for sensitive communication vulnerability in startEmailValidationActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	CVE-2023-42547
samsung -- account	Use of implicit intent for sensitive communication vulnerability in startMandatoryCheckActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	CVE-2023-42548
samsung -- account	Use of implicit intent for sensitive communication vulnerability in startNameValidationActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	CVE-2023-42549
samsung -- account	Use of implicit intent for sensitive communication vulnerability in startSignIn in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	CVE-2023-42550
samsung -- account	Use of implicit intent for sensitive communication vulnerability in startTncActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	CVE-2023-42551
samsung -- account	Improper access control vulnerability in Samsung Account prior to version 14.5.01.1 allows attackers to access sensitive information via implicit intent.	2023-11-07	5.5	CVE-2023-42540
samsung -- android	Improper Input Validation with USB Gadget Interface prior to SMR Nov-2023 Release 1 allows a physical attacker to execute arbitrary code in Kernel.	2023-11-07	6.8	CVE-2023-42533
samsung -- android	Improper input validation vulnerability in ProcessWriteFile of libsec-ril prior to SMR Nov-2023 Release 1 allows local attackers to expose sensitive information.	2023-11-07	5.5	CVE-2023-42527
samsung -- android	Improper input validation vulnerability in ChooserActivity prior to SMR Nov-2023 Release 1 allows local attackers to read arbitrary files with system privilege.	2023-11-07	5.5	CVE-2023-42534

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samsung -- easysetup	Use of implicit intent for sensitive communication vulnerability in EasySetup prior to version 11.1.13 allows attackers to get the bluetooth address of user device.	2023-11-07	5.5	CVE-2023-42555
samsung -- email	Improper authorization verification vulnerability in Samsung Email prior to version 6.1.90.4 allows attackers to read sandbox data of email.	2023-11-07	5.3	CVE-2023-42553
samsung -- health	PendingIntent hijacking vulnerability in ChallengeNotificationManager in Samsung Health prior to version 6.25 allows local attackers to access data.	2023-11-07	5.5	CVE-2023-42539
samsung -- pass	Improper Authentication vulnerabiity in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication.	2023-11-07	6.8	CVE-2023-42554
samsung -- push_service	Improper authorization in PushClientProvider of Samsung Push Service prior to version 3.4.10 allows attacker to access unique id.	2023-11-07	5.3	CVE-2023-42541
samsung -- quick_share	Improper access control vulnerability in Quick Share prior to 13.5.52.0 allows local attacker to access local files.	2023-11-07	5.5	CVE-2023-42544
samsung -- ue40d7000_firmware	Improper Restriction of Excessive Authentication Attempts vulnerability in Samsung Smart TV UE40D7000 version T-GAPDEUC-1033.2 and before allows attackers to cause a denial of service via WPS attack tools.	2023-11-08	4.3	CVE-2023-41270
sfu -- pkp_web_application_library	Missing Authorization in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	2023-11-07	5.4	CVE-2023-5900
sfu -- pkp_web_application_library	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	2023-11-07	5.4	CVE-2023-5903
sfu -- pkp_web_application_library	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	2023-11-07	5.4	CVE-2023-5904
sfu -- pkp_web_application_library	PKP-WAL (aka PKP Web Application Library or pkp-lib) before 3.3.0-16, as used in Open Journal Systems (OJS) and other products, does not verify that the file named in an XML document (used for the native import/export plugin) is an image file, before trying to use it for an issue cover image.	2023-11-06	5.3	CVE-2023-47271 MISC
sfu -- pkp_web_application_library	Unrestricted Upload of File with Dangerous Type in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	2023-11-07	4.8	CVE-2023-5901
sigstore -- cosign	Cosign is a sigstore signing tool for OCI containers. Cosign is susceptible to a denial of service by an attacker-controlled registry. An attacker who controls a remote registry can return a high number of attestations and/or signatures to Cosign and cause Cosign to enter a long loop resulting in an endless data attack. The root cause is that Cosign loops through all attestations fetched from the remote registry in pkg/cosign.FetchAttestations. The attacker needs to compromise the registry or make a request to a registry they control. When doing so, the attacker must return a high number of attestations in the response to Cosign. The result will be that the attacker can cause Cosign to go into a long or infinite loop that will prevent other users from verifying their data. In Kyvernos case, an attacker whose privileges are limited to making requests to the cluster can make a request with an image	2023-11-07	5.3	CVE-2023-46737

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reference to their own registry, trigger the infinite loop and deny other users from completing their admission requests. Alternatively, the attacker can obtain control of the registry used by an organization and return a high number of attestations instead the expected number of attestations. The issue can be mitigated rather simply by setting a limit to the limit of attestations that Cosign will loop through. The limit does not need to be high to be within the vast majority of use cases and still prevent the endless data attack. This issue has been patched in version 2.2.1 and users are advised to upgrade.			
softing -- smartlink_sw-ht	Cross-site Scripting vulnerability in Softing smartLink SW-HT before 1.30, which allows an attacker to execute a dynamic script (JavaScript, VBScript) in the context of the application.	2023-11-06	6.1	CVE-2022-48192 MISC MISC
squid-cache -- squid	SQUID is vulnerable to HTTP request smuggling, caused by chunked decoder lenience, allows a remote attacker to perform Request/Response smuggling past firewall and frontend security systems.	2023-11-03	5.3	CVE-2023-46846 MISC MISC MISC MISC MISC MISC
squidex.io -- squidex	Squidex is an open source headless CMS and content management hub. Affected versions are missing origin verification in a postMessage handler which introduces a Cross-Site Scripting (XSS) vulnerability. The editor-sdk.js file defines three different class-like functions, which employ a global message event listener: SquidexSidebar, SquidexWidget, and SquidexFormField. The registered event listener takes some action based on the type of the received message. For example, when the SquidexFormField receives a message with the type valueChanged, the value property is updated. The SquidexFormField class is for example used in the editor-editorjs.html file, which can be accessed via the public wwwroot folder. It uses the onValueChanged method to register a callback function, which passes the value provided from the message event to the editor.render. Passing an attacker-controlled value to this function introduces a Cross-Site Scripting (XSS) vulnerability.	2023-11-07	6.1	CVE-2023-46252
squidex.io -- squidex	Squidex is an open source headless CMS and content management hub. In affected versions a stored Cross-Site Scripting (XSS) vulnerability enables privilege escalation of authenticated users. The SVG element filtering mechanism intended to stop XSS attacks through uploaded SVG images, is insufficient resulting to stored XSS attacks. Squidex allows the CMS contributors to be granted the permission of uploading an SVG asset. When the asset is uploaded, a filtering mechanism is performed to validate that the SVG does not contain malicious code. The validation	2023-11-07	5.4	CVE-2023-46744

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	logic consists of traversing the HTML nodes in the DOM. In order for the validation to succeed, 2 conditions must be met: 1. No HTML tags included in a "blacklist" called "InvalidSvgElements" are present. This list only contains the element "script". and 2. No attributes of HTML tags begin with "on" (i.e. onerror, onclick) (line 65). If either of the 2 conditions is not satisfied, validation fails and the file/asset is not uploaded. However it is possible to bypass the above filtering mechanism and execute arbitrary JavaScript code by introducing other HTML elements such as an <iframe> element with a "src" attribute containing a "javascript:" value. Authenticated adversaries with the "assets.create" permission, can leverage this vulnerability to upload a malicious SVG as an asset, targeting any registered user that will attempt to open/view the asset through the Squidex CMS.			
synology -- ssl_vpn_client	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in cgi component in Synology SSL VPN Client before 1.4.7-0687 allows local users to conduct denial-of-service attacks via unspecified vectors.	2023-11-07	5.5	CVE-2023-5748
teamamaze -- amaze_file_utilities	Improper Authorization in GitHub repository teamamaze/amazefileutilities prior to 1.91.	2023-11-03	5.5	CVE-2023-5948 MISC MISC
timeteccloud -- auto_web-based_database_ management_system	Cross Site Scripting vulnerability in timetec AWDMS v.2.0 allows an attacker to obtain sensitive information via a crafted payload to the remark parameter of the New Zone function.	2023-11-08	5.4	CVE-2023-46483
urbackup -- urbackup_server	UrBackup Server 2.5.31 allows brute-force enumeration of user accounts because a failure message confirms that a username is not valid.	2023-11-07	5.3	CVE-2023-47102
veeam -- one	A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service. Note: The criticality of this vulnerability is reduced as it requires interaction by a user with the Veeam ONE Administrator role.	2023-11-07	5.4	CVE-2023-38549
veeam -- one	A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service.	2023-11-07	4.3	CVE-2023-38548
veeam -- one	A vulnerability in Veeam ONE allows a user with the Veeam ONE Read-Only User role to view the Dashboard Schedule. Note: The criticality of this vulnerability is reduced because the user with the Read-Only role is only able to view the schedule and cannot make changes.	2023-11-07	4.3	CVE-2023-41723
visser -- store_exporter_for_woocommerce	Unauth. Reflected Cross-Site Scripting') vulnerability in Visser Labs Store Exporter for WooCommerce - Export Products, Export Orders, Export Subscriptions, and More plugin <= 2.7.2 versions.	2023-11-06	6.1	CVE-2023-46822 MISC
wisdomgarden -- tronclass_ilearn	NCSIST ManageEngine Mobile Device Manager(MDM) APP's special function has a path traversal vulnerability. An unauthenticated remote	2023-11-03	6.5	CVE-2023-41356 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can exploit this vulnerability to bypass authentication and read arbitrary system files.			
wondercms -- wondercms	Cross Site Scripting vulnerability in Wonder CMS v.3.2.0 thru v.3.4.2 allows a remote attacker to execute arbitrary code via a crafted script uploaded to the installModule component.	2023-11-07	6.1	CVE-2023-41425
wordpress -- wordpress	The Front End PM WordPress plugin before 11.4.3 does not block listing the contents of the directories where it stores attachments to private messages, allowing unauthenticated visitors to list and download private attachments if the autoindex feature of the web server is enabled.	2023-11-06	6.5	CVE-2023-4930 MISC
wordpress -- wordpress	The WD WidgetTwitter plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 1.0.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2023-11-07	6.5	CVE-2023-5709
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Kathy Darling Simple User Listing plugin <= 1.9.2 versions.	2023-11-08	6.1	CVE-2023-32298
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Enej Bajgoric / Gagan Sandhu / CTLT DEV User Avatar plugin <= 1.4.11 versions.	2023-11-08	6.1	CVE-2023-46621
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FLOWFACT WP Connector plugin <= 2.1.7 versions.	2023-11-08	6.1	CVE-2023-46626
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ashish Ajani WordPress Simple HTML Sitemap plugin <= 2.1 versions.	2023-11-08	6.1	CVE-2023-46627
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPSolutions-HQ WPDBSpringClean plugin <= 1.6 versions.	2023-11-07	6.1	CVE-2023-47510
wordpress -- wordpress	The Awesome Support WordPress plugin before 6.1.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	2023-11-06	6.1	CVE-2023-5354 MISC
wordpress -- wordpress	The Digirisk plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'current_group_id' parameter in version 6.0.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2023-11-03	6.1	CVE-2023-5946 MISC MISC
wordpress -- wordpress	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in simonpedge Slide Anything - Responsive Content / HTML Slider and Carousel plugin <= 2.4.9 versions.	2023-11-07	5.4	CVE-2023-28499
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Jens Kuerschner Add to	2023-11-08	5.4	CVE-2023-46613

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Calendar Button plugin <= 1.5.1 versions.			
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in D. Relton Medialist plugin <= 1.3.9 versions.	2023-11-08	5.4	CVE-2023-46640
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Chris Yee MomentoPress for Momento360 plugin <= 1.0.1 versions.	2023-11-06	5.4	CVE-2023-46782 MISC
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Bright Plugins Pre-Orders for WooCommerce plugin <= 1.2.13 versions.	2023-11-06	5.4	CVE-2023-46783 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Yakir Sitbon, Ariel Klikstein Linker plugin <= 1.2.1 versions.	2023-11-06	5.4	CVE-2023-47177 MISC
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Apollo13Themes Apollo13 Framework Extensions plugin <= 1.9.0 versions.	2023-11-08	5.4	CVE-2023-47190
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Vyas Dipen Top 25 Social Icons plugin <= 3.1 versions.	2023-11-08	5.4	CVE-2023-47229
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Bainternet ShortCodes UI plugin <= 1.9.8 versions.	2023-11-08	5.4	CVE-2023-47231
wordpress -- wordpress	The Social Sharing Plugin - Social Warfare plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'social_warfare' shortcode in versions up to, and including, 4.4.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-4842
wordpress -- wordpress	The Simple Like Page Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sfp-page-plugin' shortcode in versions up to, and including, 1.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-4888
wordpress -- wordpress	The Ziteboard Online Whiteboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ziteboard' shortcode in versions up to, and including, 2.9.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5076
wordpress -- wordpress	The ImageMapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'imagemap' shortcode in versions up to, and including, 1.2.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to	2023-11-07	5.4	CVE-2023-5507

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
wordpress -- wordpress	The QR Code Tag plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'qrcodetag' shortcode in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5567
wordpress -- wordpress	The Bitly's plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpbitly' shortcode in all versions up to, and including, 2.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5577
wordpress -- wordpress	The WP MapIt plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wp_mapit' shortcode in all versions up to, and including, 2.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5658
wordpress -- wordpress	The Interact: Embed A Quiz On Your Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'interact-quiz' shortcode in all versions up to, and including, 3.0.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5659
wordpress -- wordpress	The SendPress Newsletters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.22.3.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5660
wordpress -- wordpress	The Social Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'socialfeed' shortcode in all versions up to, and including, 1.5.4.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions	2023-11-07	5.4	CVE-2023-5661

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
wordpress -- wordpress	The Featured Image Caption plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode and post meta in all versions up to, and including, 0.8.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5669
wordpress -- wordpress	The Gift Up Gift Cards for WordPress and WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'giftup' shortcode in all versions up to, and including, 2.20.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5703
wordpress -- wordpress	The SEO Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'slider' shortcode and post meta in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-03	5.4	CVE-2023-5707 MISC MISC MISC MISC
wordpress -- wordpress	The Telephone Number Linker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'telnumlink' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-11-07	5.4	CVE-2023-5743
wordpress -- wordpress	The video carousel slider with lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the responsive_video_gallery_with_ lightbox_video_management_func() function. This makes it possible for unauthenticated attackers to delete videos hosted from the video slider via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-11-03	5.4	CVE-2023-5945 MISC MISC MISC
wordpress -- wordpress	The UpdraftPlus: WordPress Backup & Migration Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.23.10. This is due to a lack of nonce validation and insufficient validation of the	2023-11-07	5.4	CVE-2023-5982

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	instance_id on the 'updraftmethod-googledrive-auth' action used to update Google Drive remote storage location. This makes it possible for unauthenticated attackers to modify the Google Drive location that backups are sent to via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This can make it possible for attackers to receive backups for a site which may contain sensitive information.			
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pixelgrade Comments Ratings plugin <= 1.1.7 versions.	2023-11-06	4.8	CVE-2023-23702 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Michael Mann Simple Site Verify plugin <= 1.0.7 versions.	2023-11-09	4.8	CVE-2023-36688
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in sahumedia SAHU TikTok Pixel for E-Commerce plugin <= 1.2.2 versions.	2023-11-08	4.8	CVE-2023-46642
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Om Ak Solutions Slick Popup: Contact Form 7 Popup Plugin plugin <= 1.7.14 versions.	2023-11-06	4.8	CVE-2023-46824 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Martin Gibson IdeaPush plugin <= 8.52 versions.	2023-11-08	4.8	CVE-2023-47181
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Proper Fraction LLC. Admin Bar & Dashboard Access Control plugin <= 1.2.8 versions.	2023-11-06	4.8	CVE-2023-47184 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP Map Plugins Basic Interactive World Map plugin <= 2.0 versions.	2023-11-08	4.8	CVE-2023-47223
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Post Sliders & Post Grids plugin <= 1.0.20 versions.	2023-11-08	4.8	CVE-2023-47226
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Web-Settler Social Feed | All social media in one place plugin <= 1.5.4.6 versions.	2023-11-08	4.8	CVE-2023-47227
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Muneeb Layer Slider plugin <= 1.1.9.7 versions.	2023-11-08	4.8	CVE-2023-47228
wordpress -- wordpress	The Responsive Pricing Table WordPress plugin before 5.1.8 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2023-11-06	4.8	CVE-2023-4810 MISC MISC
wordpress -- wordpress	The Simple Table Manager WordPress plugin through 1.5.6 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2023-11-06	4.8	CVE-2023-4858 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WP Discord Invite WordPress plugin before 2.5.2 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2023-11-06	4.8	CVE-2023-5181 MISC
wordpress -- wordpress	The User Registration WordPress plugin before 3.0.4.2 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2023-11-06	4.8	CVE-2023-5228 MISC
wordpress -- wordpress	The Ninja Forms Contact Form WordPress plugin before 3.6.34 does not sanitize and escape its label fields, which could allow high privilege users such as admin to perform Stored XSS attacks. Only users with the unfiltered_html capability can perform this, and such users are already allowed to use JS in posts/comments etc. however the vendor acknowledged and fixed the issue	2023-11-06	4.8	CVE-2023-5530 MISC MISC
wordpress -- wordpress	The URL Shortify WordPress plugin through 1.7.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2023-11-06	4.8	CVE-2023-5605 MISC
wordpress -- wordpress	The Amazonify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.8.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. However, please note that this can also be combined with CVE-2023-5818 for CSRF to XSS.	2023-11-07	4.8	CVE-2023-5819
wordpress -- wordpress	The Awesome Support WordPress plugin before 6.1.5 does not correctly authorize the wpas_edit_reply function, allowing users to edit posts for which they do not have permission.	2023-11-06	4.3	CVE-2023-5352 MISC
wordpress -- wordpress	The ImageMapper plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'imgmap_delete_area_ajax' function in versions up to, and including, 1.2.6. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete arbitrary posts and pages.	2023-11-07	4.3	CVE-2023-5506
wordpress -- wordpress	The ImageMapper plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.6. This is due to missing or incorrect nonce validation on the 'imgmap_save_area_title' function. This makes it possible for unauthenticated attackers to update the post title and inject malicious JavaScript via a	2023-11-07	4.3	CVE-2023-5532

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	forged request, granted they can trick a site administrator into performing an action such as clicking on a link.			
wordpress -- wordpress	The Amazonify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.8.1. This is due to missing or incorrect nonce validation on the amazonifyOptionsPage() function. This makes it possible for unauthenticated attackers to update the plugins settings, including the Amazon Tracking ID, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-11-07	4.3	CVE-2023-5818
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	2023-11-07	4.3	CVE-2023-5902
wordpress -- wordpress	The ImageMapper plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.6. This is due to missing or incorrect nonce validation on multiple functions. This makes it possible for unauthenticated attackers to update the plugin settings via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	2023-11-07	4.3	CVE-2023-5975
wpn-xm -- wpn-xm	A Cross-Site Scripting vulnerability has been detected in WPN-XM Serverstack affecting version 0.8.6. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload through the /tools/webinterface/index.php parameter and retrieve the cookie session details of an authenticated user, resulting in a session hijacking.	2023-11-03	6.1	CVE-2023-4592 MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to reflected cross-site scripting (RXSS) via the \`rev\` parameter that is used in the content of the content menu without escaping. If an attacker can convince a user to visit a link with a crafted parameter, this allows the attacker to execute arbitrary actions in the name of the user, including remote code (Groovy) execution in the case of a user with programming right, compromising the confidentiality, integrity and availability of the whole XWiki installation. This has been patched in XWiki 15.6 RC1, 15.5.1 and 14.10.14. The patch in commit \`04e325d57\` can be manually applied without upgrading (or restarting) the instance. Users are advised to upgrade or to manually apply the patch. There are no known workarounds for this vulnerability.	2023-11-06	6.1	CVE-2023-46732 MISC MISC MISC
xwiki -- xwiki	XWiki Platform is a generic wiki platform. In org.xwiki.platform:xwiki-platform-livetable-ui starting with version 3.5-milestone-1 and prior to versions 14.10.9 and 15.3-rc-1, the mail obfuscation configuration was not fully taken into account and is was still possible by obfuscated emails. This has been patched in XWiki 14.10.9 and XWiki 15.3-rc-1. A workaround is to modify the page \`XWiki.LiveTableResultsMacros\` following the patch.	2023-11-07	4.3	CVE-2023-38509

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
yugabyte -- yugabytedb	YugabyteDB is vulnerable to cross site scripting (XSS) via log injection. Writing invalidated user input to log files can allow an unprivileged attacker to forge log entries or inject malicious content into the logs.	2023-11-08	6.1	CVE-2023-6002
zohocorp -- manageengine_desktop_central	A CRLF injection vulnerability has been found in ManageEngine Desktop Central affecting version 9.1.0. This vulnerability could allow a remote attacker to inject arbitrary HTTP headers and perform HTTP response splitting attacks via the fileName parameter in /STATE_ID/1613157927228/InvSWMetering.csv.	2023-11-03	6.1	CVE-2023-4767 MISC
zohocorp -- manageengine_desktop_central	A CRLF injection vulnerability has been found in ManageEngine Desktop Central affecting version 9.1.0. This vulnerability could allow a remote attacker to inject arbitrary HTTP headers and perform HTTP response splitting attacks via the fileName parameter in /STATE_ID/1613157927228/InvSWMetering.pdf.	2023-11-03	6.1	CVE-2023-4768 MISC
zscaler -- client_connector	Origin Validation Error vulnerability in Zscaler Client Connector on Linux allows Privilege Abuse. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	2023-11-06	6.5	CVE-2023-28794 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nokia -- g-040w-q_firmware	Chunghwa Telecom NOKIA G-040W-Q Firewall function does not block ICMP TIMESTAMP requests by default, an unauthenticated remote attacker can exploit this vulnerability by sending a crafted package, resulting in partially sensitive information exposed to an actor.	2023-11-03	3.3	CVE-2023-41354 MISC
opensc -- opensc	An out-of-bounds read vulnerability was found in OpenSC packages within the MyEID driver when handling symmetric key encryption. Exploiting this flaw requires an attacker to have physical access to the computer and a specially crafted USB device or smart card. This flaw allows the attacker to manipulate APDU responses and potentially gain unauthorized access to sensitive data, compromising the system's security.	2023-11-06	3.8	CVE-2023-4535 MISC MISC MISC MISC MISC MISC
samsung -- firewall	Implicit intent hijacking vulnerability in Firewall application prior to versions 12.1.00.24 in Android 11, 13.1.00.16 in Android 12 and 14.1.00.7 in Android 13 allows 3rd party application to tamper the database of Firewall.	2023-11-07	3.3	CVE-2023-42552
samsung -- push_service	Improper access control vulnerability in Samsung Push Service prior to 3.4.10 allows local attackers to get register ID to identify the device.	2023-11-07	3.3	CVE-2023-42542

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- pyarrow	Deserialization of untrusted data in IPC and Parquet readers in PyArrow versions 0.14.0 to 14.0.0 allows arbitrary code execution. An application is vulnerable if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example user-supplied input files). This vulnerability only affects PyArrow, no other Apache Arrow implementations or bindings. It is recommended that users of PyArrow upgrade to 14.0.1. Similarly, it is recommended that downstream libraries upgrade their dependency requirements to PyArrow 14.0.1 or later. PyPI packages are already available, and we hope that conda-forge packages will be available soon. If it is not possible to upgrade, we provide a separate package `pyarrow-hotfix` that disables the vulnerability on older PyArrow versions. See https://pypi.org/project/pyarrow-hotfix/ for instructions.	2023-11-09	not yet calculated	CVE-2023-47248
apache -- uima_java_sdk_core	Deserialization of Untrusted Data, Improper Input Validation vulnerability in Apache UIMA Java SDK, Apache UIMA Java SDK, Apache UIMA Java SDK, Apache UIMA Java SDK.This issue affects Apache UIMA Java SDK: before 3.5.0. Users are recommended to upgrade to version 3.5.0, which fixes the issue. There are several locations in the code where serialized Java objects are deserialized without verifying the data. This affects in particular: * the deserialization of a Java-serialized CAS, but also other binary CAS formats that include TSI information using the CasIOUtils class; * the CAS Editor Eclipse plugin which uses the the CasIOUtils class to load data; * the deserialization of a Java-serialized CAS of the Vinci Analysis Engine service which can receive using Java-serialized CAS objects over network connections; * the CasAnnotationViewerApplet and the CasTreeViewerApplet; * the checkpointing feature of the CPE module. Note that the UIMA framework by default does not start any remotely accessible services (i.e. Vinci) that would be vulnerable to this issue. A user or developer would need to make an active choice to start such a service. However, users or developers may use the CasIOUtils in their own applications and services to parse serialized CAS data. They are affected by this issue unless they ensure that the data passed to CasIOUtils is not a serialized Java object. When using Vinci or using CasIOUtils in own services/applications, the unrestricted deserialization of Java-serialized CAS files may allow arbitrary (remote) code execution. As a remedy, it is possible to set up a global or context-specific ObjectInputFilter (cf. https://openjdk.org/jeps/290 and https://openjdk.org/jeps/415) if running UIMA on a Java version that supports it. Note that Java 1.8	2023-11-08	not yet calculated	CVE-2023-39913

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	does not support the ObjectInputFilter, so there is no remedy when running on this out-of-support platform. An upgrade to a recent Java version is strongly recommended if you need to secure an UIMA version that is affected by this issue. To mitigate the issue on a Java 9+ platform, you can configure a filter pattern through the "jdk.serialFilter" system property using a semicolon as a separator: To allow deserializing Java-serialized binary CASes, add the classes: * org.apache.uima.cas.impl.CASCompleteSerializer * org.apache.uima.cas.impl.CASMgrSerializer * org.apache.uima.cas.impl.CASSerializer * java.lang.String To allow deserializing CPE Checkpoint data, add the following classes (and any custom classes your application uses to store its checkpoints): * org.apache.uima.collection. impl.cpm.CheckpointData * org.apache.uima.util. ProcessTrace * org.apache.uima.util.impl. ProcessTrace_impl * org.apache.uima.collection. base_cpm.SynchPoint Make sure to use "!*" as the final component to the filter pattern to disallow deserialization of any classes not listed in the pattern. Apache UIMA 3.5.0 uses tightly scoped ObjectInputFilters when reading Java-serialized data depending on the type of data being expected. Configuring a global filter is not necessary with this version.			
apereo_foundation -- apereo_cas	Improper Authentication vulnerability in Apereo CAS in jakarta.servlet.http.HttpServletRequest. getRemoteAddr method allows Multi-Factor Authentication bypass. This issue affects CAS: through 7.0.0-RC7. It is unknown whether in new versions the issue will be fixed. For the date of publication there is no patch, and the vendor does not treat it as a vulnerability.	2023-11-09	not yet calculated	CVE-2023-4612
appsanywhere -- appsanywhere	The AppsAnywhere macOS client-privileged helper can be tricked into executing arbitrary commands with elevated permissions by a local user process.	2023-11-09	not yet calculated	CVE-2023-41138
appsanywhere -- appsanywhere	Symmetric encryption used to protect messages between the AppsAnywhere server and client can be broken by reverse engineering the client and used to impersonate the AppsAnywhere server.	2023-11-09	not yet calculated	CVE-2023-41137
avast/avg -- avast/avg_antivirus	A time-of-check to time-of-use (TOCTOU) bug in handling of IOCTL (input/output control) requests. This TOCTOU bug leads to an out-of-bounds write vulnerability which can be further exploited, allowing an attacker to gain full local privilege escalation on the system. This issue affects Avast/Avg Antivirus: 23.8.	2023-11-08	not yet calculated	CVE-2023-5760
axios -- axios	An issue discovered in Axios 1.5.1 inadvertently reveals the confidential XSRF-TOKEN stored in cookies by including it in the HTTP header X-XSRF-TOKEN for every request made to any host allowing attackers to view sensitive information.	2023-11-08	not yet calculated	CVE-2023-45857
bigbluebutton -- bigbluebutton	When duplicating a BigBlueButton activity, the original meeting ID was also duplicated instead of using a new ID for the new activity. This could provide unintended access to the original meeting.	2023-11-09	not yet calculated	CVE-2023-5543

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bigbluebutton -- bigbluebutton	PILOS is an open source front-end for BigBlueButton servers with a built-in load balancer. The password reset component deployed within PILOS uses the hostname supplied within the request host header when building a password reset URL. It may be possible to manipulate the URL sent to PILOS users so that it points to the attacker's server, thereby disclosing the password reset token if/when the link is followed. This only affects local user accounts and requires the password reset option to be enabled. This issue has been patched in version 2.3.0.	2023-11-08	not yet calculated	CVE-2023-47107
beijing_baichuo -- smart_s85f_firmware	A vulnerability, which was classified as problematic, was found in Beijing Baichuo Smart S85F Management Platform V31R02B10-01. Affected is an unknown function of the file /login.php. The manipulation of the argument txt_newpwd leads to weak password recovery. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-244992. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-11-11	not yet calculated	CVE-2023-5959
chromedriver -- chromedriver	Versions of the package chromedriver before 119.0.1 are vulnerable to Command Injection when setting the chromedriver.path to an arbitrary system binary. This could lead to unauthorized access and potentially malicious actions on the host system. **Note:** An attacker must have access to the system running the vulnerable chromedriver library to exploit it. The success of exploitation also depends on the permissions and privileges of the process running chromedriver.	2023-11-09	not yet calculated	CVE-2023-26156
combodo -- itop	Cross Site Scripting vulnerability in Combodo iTop v.3.1.0-2-11973 allows a local attacker to obtain sensitive information via a crafted script to the attrib_manager_id parameter in the General Information page and the id parameter in the contact page.	2023-11-09	not yet calculated	CVE-2023-47488
combodo -- itop	An issue in Combodo iTop v.3.1.0-2-11973 allows a local attacker to execute arbitrary code via a crafted script to the export-v2.php and ajax.render.php components.	2023-11-09	not yet calculated	CVE-2023-47489
couchbase_inc. -- couchbase_server	An issue was discovered in Couchbase Server 7.2.0. There is a private key leak in debug.log while adding a pre-7.0 node to a 7.2 cluster.	2023-11-08	not yet calculated	CVE-2023-45875
discourse -- discourse	Discourse is an open source platform for community discussion. In versions 3.1.0 through 3.1.2 of the `stable` branch and versions 3.1.0,beta6 through 3.2.0.beta2 of the `beta` and `tests-passed` branches, Redis memory can be depleted by crafting a site with an abnormally long favicon URL and drafting multiple posts which Onebox it. The issue is patched in version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.	2023-11-10	not yet calculated	CVE-2023-47120

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
discourse -- discourse	Discourse is an open source platform for community discussion. Prior to version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches, the embedding feature is susceptible to server-side request forgery. The issue is patched in version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches. As a workaround, disable the Embedding feature.	2023-11-10	not yet calculated	CVE-2023-47121
discourse -- discourse	Discourse is an open source platform for community discussion. Prior to version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches, if a user has been quoted and uses a `|` in their full name, they might be able to trigger a bug that generates a lot of duplicate content in all the posts they've been quoted by updating their full name again. Version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches contain a patch for this issue. No known workaround exists, although one can stop the "bleeding" by ensuring users only use alphanumeric characters in their full name field.	2023-11-10	not yet calculated	CVE-2023-45806
discourse -- discourse	Discourse is an open source platform for community discussion. Prior to version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches, there is an edge case where a bookmark reminder is sent and an unread notification is generated, but the underlying bookmarkable (e.g. post, topic, chat message) security has changed, making it so the user can no longer access the underlying resource. As of version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches, bookmark reminders are now no longer sent if the user does not have access to the underlying bookmarkable, and also the unread bookmark notifications are always filtered by access. There are no known workarounds.	2023-11-10	not yet calculated	CVE-2023-45816
discourse -- discourse	Discourse is an open source platform for community discussion. Prior to version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches, some theme components allow users to add svgs with unlimited `height` attributes, and this can affect the availability of subsequent replies in a topic. Most Discourse instances are unaffected, only instances with the svgbob or the mermaid theme component are within scope. The issue is patched in version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches. As a workaround, disable or remove the relevant theme components.	2023-11-10	not yet calculated	CVE-2023-46130
discourse -- discourse	Discourse is an open source platform for community discussion. Prior to version 3.1.3 of the `stable` branch and version 3.2.0.beta3 of the `beta` and `tests-passed` branches, some links can inject arbitrary HTML tags when rendered through our Onebox engine. The issue is patched in version 3.1.3 of the `stable` branch and version	2023-11-10	not yet calculated	CVE-2023-47119

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3.2.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.			
eclipse_foundation -- eclipse_ide	In Eclipse IDE versions < 2023-09 (4.29) some files with xml content are parsed vulnerable against all sorts of XXE attacks. The user just needs to open any evil project or update an open project with a vulnerable file (for example for review a foreign repository or patch).	2023-11-09	not yet calculated	CVE-2023-4218
ethyca -- fides	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in your runtime environment, and the enforcement of privacy regulations in your code. The Fides web application allows data subject users to request access to their personal data. If the request is approved by the data controller user operating the Fides web application, the data subject's personal data can then be retrieved from connected systems and data stores before being bundled together as a data subject access request package for the data subject to download. Supported data formats for the package include json and csv, but the most commonly used format is a series of HTML files compressed in a ZIP file. Once downloaded and unzipped, the data subject user can browse the HTML files on their local machine. It was identified that there was no validation of input coming from e.g. the connected systems and data stores which is later reflected in the downloaded data. This can result in an HTML injection that can be abused e.g. for phishing attacks or malicious JavaScript code execution, but only in the context of the data subject's browser accessing a HTML page using the `file://` protocol. Exploitation is limited to rogue Admin UI users, malicious connected system / data store users, and the data subject user if tricked via social engineering into submitting malicious data themselves. This vulnerability has been patched in version 2.23.3.	2023-11-08	not yet calculated	CVE-2023-47114
free_software_foundation -- grub-legacy	An attacker with local access to a system (either through a disk or external drive) can present a modified XFS partition to grub-legacy in such a way to exploit a memory corruption in grub's XFS file system implementation.	2023-11-10	not yet calculated	CVE-2023-4949
freebsd -- freebsd	In versions of FreeBSD 12.4-RELEASE prior to 12.4-RELEASE-p7 and FreeBSD 13.2-RELEASE prior to 13.2-RELEASE-p5 the __sflush() stdio function in libc does not correctly update FILE objects' write space members for write-buffered streams when the write(2) system call returns an error. Depending on the nature of an application that calls libc's stdio functions and the presence of errors returned from the write(2) system call (or an overridden stdio write routine) a heap buffer overflow may occur. Such overflows may lead to data corruption or the execution of arbitrary code at the privilege level of the calling program.	2023-11-08	not yet calculated	CVE-2023-5941
freebsd -- freebsd	In versions of FreeBSD 13-RELEASE before 13-RELEASE-p5, under certain circumstances the cap_net libcasper(3) service incorrectly validates that updated constraints are strictly subsets of the	2023-11-08	not yet calculated	CVE-2023-5978

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	active constraints. When only a list of resolvable domain names was specified without setting any other limitations, an application could submit a new list of domains including include entries not previously listed. This could permit the application to resolve domain names that were previously restricted.			
gitlab -- gitlab	An issue has been discovered in GitLab EE affecting all versions starting from 15.3 prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1. Code owner approval was not removed from merge requests when the target branch was updated.	2023-11-09	not yet calculated	CVE-2023-4379
gitsign -- gitsign	Gitsign is software for keyless Git signing using Sigstore. In versions of gitsign starting with 0.6.0 and prior to 0.8.0, Rekor public keys were fetched via the Rekor API, instead of through the local TUF client. If the upstream Rekor server happened to be compromised, gitsign clients could potentially be tricked into trusting incorrect signatures. There is no known compromise the default public good instance (`rekor.sigstore.dev`) - anyone using this instance is unaffected. This issue was fixed in v0.8.0. No known workarounds are available.	2023-11-10	not yet calculated	CVE-2023-47122
go_standard_library -- path/filepath	The filepath package does not recognize paths with a \??\ prefix as special. On Windows, a path beginning with \??\ is a Root Local Device path equivalent to a path beginning with \?\. Paths with a \??\ prefix may be used to access arbitrary locations on the system. For example, the path \??\c:\x is equivalent to the more common path c:\x. Before fix, Clean could convert a rooted path such as \a\..\??\b into the root local device path \??\b. Clean will now convert this to .\??\b. Similarly, Join(\, ??, b) could convert a seemingly innocent sequence of path elements into the root local device path \??\b. Join will now convert this to \.\??\b. In addition, with fix, IsAbs now correctly reports paths beginning with \??\ as absolute, and VolumeName correctly reports the \??\ prefix as a volume name.	2023-11-09	not yet calculated	CVE-2023-45283
go_standard_library -- path/filepath	On Windows, The IsLocal function does not correctly detect reserved device names in some cases. Reserved names followed by spaces, such as "COM1 ", and reserved names "COM" and "LPT" followed by superscript 1, 2, or 3, are incorrectly reported as local. With fix, IsLocal now correctly reports these names as non-local.	2023-11-09	not yet calculated	CVE-2023-45284
gpac -- mp4box	Buffer Overflow vulnerability in gpac MP4Box v.2.3-DEV-rev573-g201320819-master allows a local attacker to cause a denial of service via the gpac/src/isomedia/isom_read.c:2807:51 function in gf_isom_get_user_data.	2023-11-07	not yet calculated	CVE-2023-46001
harbor -- harbor	A timing condition in Harbor 2.6.x and below, Harbor 2.7.2 and below, Harbor 2.8.2 and below, and Harbor 1.10.17 and below allows an attacker with network access to create jobs/stop job tasks and retrieve job task information.	2023-11-09	not yet calculated	CVE-2023-20902
hashicorp -- vault	HashiCorp Vault and Vault Enterprise inbound client requests triggering a policy check can lead	2023-11-09	not yet calculated	CVE-2023-5954

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to an unbounded consumption of memory. A large number of these requests may lead to denial-of-service. Fixed in Vault 1.15.2, 1.14.6, and 1.13.10.			
hcl_software -- hcl_connections	HCL Connections is vulnerable to reflected cross-site scripting (XSS) where an attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user after visiting the vulnerable URL which contains the malicious script code. This may allow the attacker to steal cookie-based authentication credentials and comprise a user's account then launch other attacks.	2023-11-09	not yet calculated	CVE-2023-37533
headscale -- headscale	Headscale through 0.22.3 writes bearer tokens to info-level logs.	2023-11-11	not yet calculated	CVE-2023-47390
hoteldruid -- hoteldruid	Cross-site scripting vulnerability in HOTELDRUID 3.0.5 and earlier allows a remote unauthenticated attacker to execute an arbitrary script on the web browser of the user who is logging in to the product.	2023-11-10	not yet calculated	CVE-2023-47164
huawei -- emui	Vulnerability of parameters being out of the value range in the QMI service module. Successful exploitation of this vulnerability may cause errors in reading file data.	2023-11-08	not yet calculated	CVE-2023-46772
humansignal -- label_studio	Label Studio is a multi-type data labeling and annotation tool with standardized output format. There is a vulnerability that can be chained within the ORM Leak vulnerability to impersonate any account on Label Studio. An attacker could exploit these vulnerabilities to escalate their privileges from a low privilege user to a Django Super Administrator user. The vulnerability was found to affect versions before `1.8.2`, where a patch was introduced.	2023-11-09	not yet calculated	CVE-2023-43791
ibm -- aix	IBM AIX's 7.3 Python implementation could allow a non-privileged local user to exploit a vulnerability to cause a denial of service. IBM X-Force ID: 267965.	2023-11-10	not yet calculated	CVE-2023-45167
ibm -- qradar_siem	IBM QRadar SIEM 7.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 267484.	2023-11-11	not yet calculated	CVE-2023-43057
jaspersoft -- clarity_ppm	Jaspersoft Clarity PPM version 14.3.0.298 was discovered to contain an arbitrary file upload vulnerability via the Profile Picture Upload function.	2023-11-09	not yet calculated	CVE-2023-37790
johnson_controls -- quantum_hd_unity	An unauthorized user could access debug features in Quantum HD Unity products that were accidentally exposed.	2023-11-10	not yet calculated	CVE-2023-4804
lanaccess -- onsafe_monitorhm	An improper input validation vulnerability has been found in Lanaccess ONSAFE MonitorHM affecting version 3.7.0. This vulnerability could lead a remote attacker to exploit the checkbox element and perform remote code execution, compromising the entire infrastructure.	2023-11-08	not yet calculated	CVE-2023-6012
lenovo -- 1_preload_directory	A privilege escalation vulnerability was reported in Lenovo preloaded devices deployed using	2023-11-08	not yet calculated	CVE-2023-4706

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Microsoft AutoPilot under a standard user account due to incorrect default privileges.			
lenovo -- bios	A memory leakage vulnerability was reported in the SWSMI_Shadow DXE driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	not yet calculated	CVE-2023-45075
lenovo -- bios	A memory leakage vulnerability was reported in the 534D0140 DXE driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	not yet calculated	CVE-2023-45076
lenovo -- bios	A memory leakage vulnerability was reported in the 534D0740 DXE driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	not yet calculated	CVE-2023-45077
lenovo -- bios	A memory leakage vulnerability was reported in the DustFilterAlertSmm SMM driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	not yet calculated	CVE-2023-45078
lenovo -- bios	A memory leakage vulnerability was reported in the NvmramSmm SMM driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	not yet calculated	CVE-2023-45079
lenovo -- desktop_bios	A buffer overflow was reported in the LemSecureBootForceKey module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	not yet calculated	CVE-2023-43567
lenovo -- desktop_bios	A buffer over-read was reported in the LemSecureBootForceKey module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to disclose sensitive information.	2023-11-08	not yet calculated	CVE-2023-43568
lenovo -- desktop_bios	A buffer overflow was reported in the OemSmi module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	not yet calculated	CVE-2023-43569
lenovo -- desktop_bios	A potential vulnerability was reported in the SMI callback function of the OemSmi driver that may allow a local attacker with elevated permissions to execute arbitrary code.	2023-11-08	not yet calculated	CVE-2023-43570
lenovo -- ideapad	A buffer overflow was reported in the FmpSipoCapsuleDriver driver in the IdeaPad Duet 3-10IGL5 that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	not yet calculated	CVE-2023-5075
lenovo -- lecloud_app	Lenovo LeCloud App improper input validation allows attackers to access arbitrary components and arbitrary file downloads, which could result in information disclosure.	2023-11-08	not yet calculated	CVE-2023-5079
lenovo -- system_update	An uncontrolled search path vulnerability was reported in Lenovo System Update that could allow an attacker with local access to execute code with elevated privileges.	2023-11-08	not yet calculated	CVE-2023-4632
lenovo -- thinkpad	A vulnerability was reported in some ThinkPad BIOS that could allow a physical or local attacker with elevated privileges to tamper with BIOS firmware.	2023-11-08	not yet calculated	CVE-2023-5078
lenovo -- view_driver	A potential use-after-free vulnerability was reported in the Lenovo View driver that could result	2023-11-08	not yet calculated	CVE-2023-4891

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in denial of service.			
f.b.p -- members_line	The leakage of channel access token in F.B.P members Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47363
f.b.p -- members_line	The leakage of channel access token in nagaoka taxi Line 13.6.1 allows remote attackers to send malicious notifications to victims	2023-11-09	not yet calculated	CVE-2023-47364
f.b.p -- members_line	The leakage of channel access token in Lil.OFF-PRICE STORE Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47365
f.b.p -- members_line	The leakage of channel access token in craft_members Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47366
f.b.p -- members_line	The leakage of channel access token in platinum clinic Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47367
f.b.p -- members_line	The leakage of channel access token in taketorinoyu Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47368
f.b.p -- members_line	The leakage of channel access token in best_training_member Line 13.6.1 allows remote attackers to send malicious notifications.	2023-11-09	not yet calculated	CVE-2023-47369
f.b.p -- members_line	The leakage of channel access token in bluetrick Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47370
f.b.p -- members_line	The leakage of channel access token in UPDATESALON C-LOUNGE Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47372
f.b.p -- members_line	The leakage of channel access token in DRAGON FAMILY Line 13.6.1 allows remote attackers to send malicious notifications to victims.	2023-11-09	not yet calculated	CVE-2023-47373
linux -- kernel	A use-after-free flaw was found in lan78xx_disconnect in drivers/net/usb/lan78xx.c in the network sub-component, net/usb/lan78xx in the Linux Kernel. This flaw allows a local attacker to crash the system when the LAN78XX USB device detaches.	2023-11-09	not yet calculated	CVE-2023-6039
linux -- kernel	A race condition was found in the QXL driver in the Linux kernel. The qxl_mode_dumb_create() function dereferences the qobj returned by the qxl_gem_object_create_with_handle(), but the handle is the only one holding a reference to it. This flaw allows an attacker to guess the returned handle value and trigger a use-after-free issue, potentially leading to a denial of service or privilege escalation.	2023-11-09	not yet calculated	CVE-2023-39198
loytec_electronics -- multiple_products	LOYTEC LINX-212 firmware 6.2.4 and LVIS-3ME12-A1 firmware 6.2.2 and LIOB-586 firmware 6.2.3 devices send password-change requests via cleartext HTTP.	2023-11-04	not yet calculated	CVE-2023-46380 MISC
loytec_electronics -- multiple_products	LOYTEC LINX-212 firmware 6.2.4 and LVIS-3ME12-A1 firmware 6.2.2 and LIOB-586 firmware 6.2.3 devices lack authentication for the preinstalled version of LWEB-802 via an lweb802_pre/ URI. An unauthenticated attacker	2023-11-04	not yet calculated	CVE-2023-46381 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can edit any project (or create a new project) and control its GUI.			
loytec_electronics -- multiple_products	LOYTEC LINX-212 firmware 6.2.4 and LVIS-3ME12-A1 firmware 6.2.2 and LIOB-586 firmware 6.2.3 devices use cleartext HTTP for login.	2023-11-04	not yet calculated	CVE-2023-46382 MISC
microsoft -- edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-11-10	not yet calculated	CVE-2023-36027
mldb.ai -- mldb.ai	Cross Site Scripting vulnerability in MLDB.ai v.2017.04.17.0 allows a remote attacker to execute arbitrary code via a crafted payload to the public_html/doc/index.html.	2023-11-09	not yet calculated	CVE-2023-46492
moodle -- moodle	A remote code execution risk was identified in the Lesson activity. By default, this was only available to teachers and managers.	2023-11-09	not yet calculated	CVE-2023-5539
moodle -- moodle	A remote code execution risk was identified in the IMSCP activity. By default, this was only available to teachers and managers.	2023-11-09	not yet calculated	CVE-2023-5540
moodle -- moodle	Students in "Only see own membership" groups could see other students in the group, which should be hidden.	2023-11-09	not yet calculated	CVE-2023-5542
moodle -- moodle	H5P metadata automatically populated the author with the user's username, which could be sensitive information.	2023-11-09	not yet calculated	CVE-2023-5545
moodle -- moodle	Stronger revision number limitations were required on file serving endpoints to improve cache poisoning protection.	2023-11-09	not yet calculated	CVE-2023-5548
moodle -- moodle	Insufficient web service capability checks made it possible to move categories a user had permission to manage, to a parent category they did not have the capability to manage.	2023-11-09	not yet calculated	CVE-2023-5549
moodle -- moodle	In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user who also has direct access to the web server outside of the Moodle webroot could utilize a local file include to achieve remote code execution.	2023-11-09	not yet calculated	CVE-2023-5550
moodle -- moodle	Separate Groups mode restrictions were not honored in the forum summary report, which would display users from other groups.	2023-11-09	not yet calculated	CVE-2023-5551
natus -- multiple_products	Natus NeuroWorks and SleepWorks before 8.4 GMA3 utilize a default password of xltek for the Microsoft SQL Server service sa account, allowing a threat actor to perform remote code execution, data exfiltration, or other nefarious actions such as tampering with data or destroying/disrupting MSSQL services.	2023-11-10	not yet calculated	CVE-2023-47800
okta -- ldap_agent	The LDAP Agent Update service with versions prior to 5.18 used an unquoted path, which could allow arbitrary code execution.	2023-11-08	not yet calculated	CVE-2023-0392
opentelemetry -- opentelemetry	OpenTelemetry-Go Contrib is a collection of third-party packages for OpenTelemetry-Go. Prior to version 0.46.0, the grpc Unary Server Interceptor	2023-11-10	not yet calculated	CVE-2023-47108

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	out of the box adds labels `net.peer.sock.addr` and `net.peer.sock.port` that have unbound cardinality. It leads to the server's potential memory exhaustion when many malicious requests are sent. An attacker can easily flood the peer address and port for requests. Version 0.46.0 contains a fix for this issue. As a workaround to stop being affected, a view removing the attributes can be used. The other possibility is to disable grpc metrics instrumentation by passing `otelgrpc.WithMeterProvider` option with `noop.NewMeterProvider`.			
opentext -- fortify_scancentral_dast	Incorrect Privilege Assignment vulnerability in opentext Fortify ScanCentral DAST. The vulnerability could be exploited to gain elevated privileges. This issue affects Fortify ScanCentral DAST versions 21.1, 21.2, 21.2.1, 22.1, 22.1.1, 22.2, 23.1.	2023-11-08	not yet calculated	CVE-2023-5913
openvpn -- openvpn	Using the --fragment option in certain configuration setups OpenVPN version 2.6.0 to 2.6.6 allows an attacker to trigger a divide by zero behaviour which could cause an application crash, leading to a denial of service.	2023-11-11	not yet calculated	CVE-2023-46849
openvpn -- openvpn	Use after free in OpenVPN version 2.6.0 to 2.6.6 may lead to undefined behavoir, leaking memory buffers or remote execution when sending network buffers to a remote peer.	2023-11-11	not yet calculated	CVE-2023-46850
ovh -- the_bastion	The Bastion provides authentication, authorization, traceability and auditability for SSH accesses. SCP and SFTP plugins don't honor group-based JIT MFA. Establishing a SCP/SFTP connection through The Bastion via a group access where MFA is enforced does not ask for additional factor. This abnormal behavior only applies to per-group-based JIT MFA. Other MFA setup types, such as Immediate MFA, JIT MFA on a per-plugin basis and JIT MFA on a per-account basis are not affected. This issue has been patched in version 3.14.15.	2023-11-08	not yet calculated	CVE-2023-45140
palo_alto_networks -- cortex_xsoar	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux operating system enables a local attacker to execute programs with elevated privileges if the attacker has shell access to the engine.	2023-11-08	not yet calculated	CVE-2023-3282
pfsense_ce -- pfsense_ce	An issue discovered in Pfsense CE version 2.6.0 allows attackers to compromise user accounts via weak password requirements.	2023-11-08	not yet calculated	CVE-2023-29974
pfsense_ce -- pfsense_ce	An issue discovered in Pfsense CE version 2.6.0 allows attackers to change the password of any user without verification.	2023-11-09	not yet calculated	CVE-2023-29975
philips -- encoreanywhere	The HTTP header in Philips EncoreAnywhere contains data an attacker may be able to use to gain sensitive information.	2023-11-09	not yet calculated	CVE-2018-8863
phpgurukul -- restaurant_table_booking_system	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0. It has been rated as critical. This issue affects some unknown processing of the file check-status.php of the	2023-11-10	not yet calculated	CVE-2023-6074

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	component Booking Reservation Handler. The manipulation leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-244943.			
phpgurukul -- restaurant_table_booking_system	A vulnerability classified as problematic has been found in PHPGurukul Restaurant Table Booking System 1.0. Affected is an unknown function of the file index.php of the component Reservation Request Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-244944.	2023-11-10	not yet calculated	CVE-2023-6075
phpgurukul -- restaurant_table_booking_system	A vulnerability classified as problematic was found in PHPGurukul Restaurant Table Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file booking-details.php of the component Reservation Status Handler. The manipulation of the argument bid leads to information disclosure. The attack can be launched remotely. The identifier VDB-244945 was assigned to this vulnerability.	2023-11-10	not yet calculated	CVE-2023-6076
piccolo -- piccolo	Piccolo is an object-relational mapping and query builder which supports asyncio. Prior to version 1.1.1, the handling of named transaction \`savepoints\` in all database implementations is vulnerable to SQL Injection via f-strings. While the likelihood of an end developer exposing a \`savepoints\` \`name\` parameter to a user is highly unlikely, it would not be unheard of. If a malicious user was able to abuse this functionality, they would have essentially direct access to the database and the ability to modify data to the level of permissions associated with the database user. A non-exhaustive list of actions possible based on database permissions is: Read all data stored in the database, including usernames and password hashes; insert arbitrary data into the database, including modifying existing records; and gain a shell on the underlying server. Version 1.1.1 fixes this issue.	2023-11-10	not yet calculated	CVE-2023-47128
prestashop -- blockreassurance	PrestaShop blockreassurance adds an information block aimed at offering helpful information to reassure customers that the store is trustworthy. When adding a block in blockreassurance module, a BO user can modify the http request and give the path of any file in the project instead of an image. When deleting the block from the BO, the file will be deleted. It is possible to make the website completely unavailable by removing index.php for example. This issue has been patched in version 5.1.4.	2023-11-08	not yet calculated	CVE-2023-47109
projectworlds -- online_job_portal	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'filename' parameter of the sign-up.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46676
projectworlds -- online_job_portal	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txt_uname' parameter of the sign-up.php resource	2023-11-07	not yet calculated	CVE-2023-46677

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	does not validate the characters received and they are sent unfiltered to the database.			
projectworlds -- online_job_portal	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txt_upass' parameter of the sign-up.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46678
projectworlds -- online_job_portal	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txt_uname_email' parameter of the index.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46679
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'password' parameter of the auth/auth.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46786
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the auth/auth.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46787
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter in the 'uploadphoto()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46788
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'filename' attribute of the 'pic1' multipart parameter of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46789
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'filename' attribute of the 'pic2' multipart parameter of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46790
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'filename' attribute of the 'pic4' multipart parameter of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46792
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'day' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46793
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'email' parameter in the 'register()' function of the functions.php resource	2023-11-07	not yet calculated	CVE-2023-46794

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	does not validate the characters received and they are sent unfiltered to the database.			
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'gender' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46795
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'month' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46796
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'name' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46797
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'year' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46799
projectworlds -- online_matrimonial_project	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the view_profile.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-11-07	not yet calculated	CVE-2023-46800
qnap_systems_inc. -- multiple_products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2376 build 20230421 and later QuTS hero h5.0.1.2376 build 20230421 and later QuTScloud c5.1.0.2498 and later.	2023-11-10	not yet calculated	CVE-2023-23367
qnap_systems_inc. -- qumagie	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.1.4 and later	2023-11-10	not yet calculated	CVE-2023-41284
qnap_systems_inc. -- qumagie	An OS command injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QuMagie 2.1.3 and later	2023-11-10	not yet calculated	CVE-2023-39295
qnap_systems_inc. -- qumagie	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.1.4 and later	2023-11-10	not yet calculated	CVE-2023-41285

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sentry -- sentry-javascript	sentry-javascript provides Sentry SDKs for JavaScript. An unsanitized input of Next.js SDK tunnel endpoint allows sending HTTP requests to arbitrary URLs and reflecting the response back to the user. This issue only affects users who have Next.js SDK tunneling feature enabled. The problem has been fixed in version 7.77.0.	2023-11-10	not yet calculated	CVE-2023-46729
solarwinds_ -- network_configuration_manager	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows a low-level user to perform the actions with SYSTEM privileges. We found this issue was not resolved in CVE-2023-33226	2023-11-09	not yet calculated	CVE-2023-40054
solarwinds_ -- network_configuration_manager	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows a low-level user to perform the actions with SYSTEM privileges. We found this issue was not resolved in CVE-2023-33227	2023-11-09	not yet calculated	CVE-2023-40055
spiceworks -- help_desk_server	An issue was discovered in Spiceworks Help Desk Server before 1.3.3. A Blind Boolean SQL injection vulnerability within the order_by_for_ticket function in app/models/reporting/database_query.rb allows an authenticated attacker to execute arbitrary SQL commands via the sort parameter. This can be leveraged to leak local files from the host system, leading to remote code execution (RCE) through deserialization of malicious data.	2023-11-09	not yet calculated	CVE-2021-43609
statmic -- statmic	Statmic is a core Laravel content management system Composer package. Prior to versions 3.4.13 and 4.33.0, on front-end forms with an asset upload field, PHP files crafted to look like images may be uploaded. This only affects forms using the "Forms" feature and not just _any_ arbitrary form. This does not affect the control panel. This issue has been patched in 3.4.13 and 4.33.0.	2023-11-10	not yet calculated	CVE-2023-47129
symfony -- symfony	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Starting in versions 5.4.21 and 6.2.7 and prior to versions 5.4.31 and 6.3.8, `SessionStrategyListener` does not migrate the session after every successful login. It does so only in case the logged in user changes by means of checking the user identifier. In some use cases, the user identifier doesn't change between the verification phase and the successful login, while the token itself changes from one type (partially-authenticated) to another (fully-authenticated). When this happens, the session id should be regenerated to prevent possible session fixations, which is not the case at the moment. As of versions 5.4.31 and 6.3.8, Symfony now checks the type of the token in addition to the user identifier before deciding whether the session id should be regenerated.	2023-11-10	not yet calculated	CVE-2023-46733

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
symfony -- symfony	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Starting in versions 2.0.0, 5.0.0, and 6.0.0 and prior to versions 4.4.51, 5.4.31, and 6.3.8, some Twig filters in CodeExtension use \`is_safe=html\` but don't actually ensure their input is safe. As of versions 4.4.51, 5.4.31, and 6.3.8, Symfony now escapes the output of the affected filters.	2023-11-10	not yet calculated	CVE-2023-46734
symfony -- symfony	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Starting in version 6.0.0 and prior to version 6.3.8, the error message in \`WebhookController\` returns unescaped user-submitted input. As of version 6.3.8, \`WebhookController\` now doesn't return any user-submitted input in its response.	2023-11-10	not yet calculated	CVE-2023-46735
telit_cinterion -- multiple_products	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow a remote unauthenticated attacker to execute arbitrary code on the targeted system by sending a specially crafted SMS message.	2023-11-09	not yet calculated	CVE-2023-47610
telit_cinterion -- multiple_products	A CWE-269: Improper Privilege Management vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow a local, low privileged attacker to elevate privileges to "manufacturer" level on the targeted system.	2023-11-10	not yet calculated	CVE-2023-47611
telit_cinterion -- multiple_products	A CWE-552: Files or Directories Accessible to External Parties vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow an attacker with physical access to the target system to obtain a read/write access to any files and directories on the targeted system, including hidden files and directories.	2023-11-09	not yet calculated	CVE-2023-47612
telit_cinterion -- multiple_products	A CWE-23: Relative Path Traversal vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow a local, low privileged attacker to escape from virtual directories and get read/write access to protected files on the targeted system.	2023-11-09	not yet calculated	CVE-2023-47613
telit_cinterion -- multiple_products	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow a local, low privileged attacker to disclose hidden virtual paths and file names on the targeted system.	2023-11-10	not yet calculated	CVE-2023-47614
telit_cinterion -- multiple_products	A CWE-526: Exposure of Sensitive Information Through Environmental Variables vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow a	2023-11-09	not yet calculated	CVE-2023-47615

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	local, low privileged attacker to get access to a sensitive data on the targeted system.			
telit_cinterion -- multiple_products	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Telit Cinterion BGS5, Telit Cinterion EHS5/6/8, Telit Cinterion PDS5/6/8, Telit Cinterion ELS61/81, Telit Cinterion PLS62 that could allow an attacker with physical access to the target system to get access to a sensitive data on the targeted system.	2023-11-09	not yet calculated	CVE-2023-47616
tibco_software_inc. -- spotfire	The Spotfire Connectors component of TIBCO Software Inc.'s Spotfire Analyst, Spotfire Server, and Spotfire for AWS Marketplace contains an easily exploitable vulnerability that allows a low privileged attacker with read/write access to craft malicious Analyst files. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s Spotfire Analyst: versions 12.3.0, 12.4.0, and 12.5.0, Spotfire Server: versions 12.3.0, 12.4.0, and 12.5.0, and Spotfire for AWS Marketplace: version 12.5.0.	2023-11-08	not yet calculated	CVE-2023-26221
tongda -- oa	A vulnerability classified as critical has been found in Tongda OA 2017 up to 11.9. Affected is an unknown function of the file general/system/censor_words/module/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-244872. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-11-09	not yet calculated	CVE-2023-6052
tongda -- oa	A vulnerability, which was classified as critical, has been found in Tongda OA 2017 up to 11.9. Affected by this issue is some unknown functionality of the file general/system/censor_words/manage/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-244874 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-11-09	not yet calculated	CVE-2023-6053
tongda -- oa	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file general/wiki/cp/manage/lock.php. The manipulation of the argument TERM_ID_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-244875. NOTE: The vendor	2023-11-09	not yet calculated	CVE-2023-6054

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	was contacted early about this disclosure but did not respond in any way.			
volkswagen -- id.3	Attacker can perform a Denial-of-Service attack to crash the ICAS 3 IVI ECU in a Volkswagen ID.3 (and other vehicles of the VW Group with the same hardware) and spoof volume setting commands to irreversibly turn on audio volume to maximum via REST API calls.	2023-11-10	not yet calculated	CVE-2023-6073
wbce_cms -- wbce_cms	SQL injection vulnerability in the miniform module in WBCE CMS v.1.6.0 allows remote unauthenticated attacker to execute arbitrary code via the DB_RECORD_TABLE parameter.	2023-11-10	not yet calculated	CVE-2023-39796
wildfly-core -- wildfly-core	A flaw was found in wildfly-core. A management user could use the resolve-expression in the HAL Interface to read possible sensitive information from the Wildfly system. This issue could allow a malicious user to access the system and obtain possible sensitive information from the system.	2023-11-08	not yet calculated	CVE-2023-4061
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in ReCorp Export WP Page to Static HTML/CSS plugin <= 2.1.9 versions.	2023-11-10	not yet calculated	CVE-2023-31077
xwiki -- xwiki	application-collabora is an integration of Collabora Online in XWiki. As part of the application use cases, depending on the rights that a user has over a document, they should be able to open the office attachments files in view or edit mode. Currently, if a user opens an attachment file in edit mode in collabora, this right will be preserved for all future users, until the editing session is closes, even if some of them have only view right. Collabora server is the one issuing this request and it seems that the `userCanWrite` query parameter is cached, even if, for example, token is not. This issue has been patched in version 1.3.	2023-11-09	not yet calculated	CVE-2023-46743
yugabytedb -- yugabytedb_anywhere	Prometheus metrics are available without authentication. These metrics expose detailed and sensitive information about the YugabyteDB Anywhere environment.	2023-11-08	not yet calculated	CVE-2023-6001
zitadel -- zitadel	ZITADEL provides identity infrastructure. ZITADEL provides administrators the possibility to define a `Lockout Policy` with a maximum amount of failed password check attempts. On every failed password check, the number of failed checks is compared against the configured maximum. Exceeding the limit, will lock the user and prevent further authentication. In the affected implementation it was possible for an attacker to start multiple parallel password checks, giving him the possibility to try out more combinations than configured in the `Lockout Policy`. This vulnerability has been patched in versions 2.40.5 and 2.38.3.	2023-11-08	not yet calculated	CVE-2023-47111
zyxel -- gs1900-24ep	The improper privilege management vulnerability in the Zyxel GS1900-24EP switch firmware version V2.70(ABTO.5) could allow an authenticated local user with read-only access to modify system settings on a vulnerable device.	2023-11-07	not yet calculated	CVE-2023-35140

Back to top FYI But I promise not to send it again.

This product is provided subject to this Notification and this Privacy & Use policy.

Menu

SHARE:

Vulnerability Summary for the Week of October 23, 2023

Released: Oct 30, 2023

Document ID: SB23-303

The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology <https://www.nist.gov/> (NIST) National Vulnerability Database <https://nvd.nist.gov/> (NVD) in the past week. NVD is sponsored by CISA. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Vulnerabilities are based on the Common Vulnerabilities and Exposures <https://cve.mitre.org/> (CVE) vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System <https://nvd.nist.gov/cvss.cfm> (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- High: vulnerabilities with a CVSS base score of 7.0–10.0
- Medium: vulnerabilities with a CVSS base score of 4.0–6.9
- Low: vulnerabilities with a CVSS base score of 0.0–3.9

Entries may include additional information provided by organizations and efforts sponsored by CISA. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletin is compiled from external, open-source reports and is not a direct result of CISA analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'fnm' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-26	9.8	CVE-2023-43737 MISC <https://https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'email' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-27	9.8	CVE-2023-43738 MISC <https://https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'contact' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-27	9.8	CVE-2023-44162 MISC <https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'lnm' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-26	9.8	CVE-2023-44267 MISC <https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'gender' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-26	9.8	CVE-2023-44268 MISC <https://https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'add1' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-27	9.8	CVE-2023-44375 MISC <https://https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'add2' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-27	9.8	CVE-2023-44376 MISC <https://https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>
projectworlds_pvt._limited -- online_art_gallery	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'add3' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-27	9.8	CVE-2023-44377 MISC <https://https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/ono>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- http_server	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.57.	2023-10-23	9.1	CVE-2023-31122 MISC <https://httpd.apache.org/security/vulnerabilities_24.html> MISC <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ti3v2yceum65qdypggnuz7uonim5oexc/> MISC <https://security.netapp.com/advisory/ntap-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				20231027-0011/>
byzoro -- smart_s85f_firmware	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20231010 and classified as critical. This issue affects some unknown processing of the file /sysmanage/importconf.php. The manipulation of the argument btn_file_renew leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-21	9.8	CVE-2023-5683 MISC <https://github.com/yaphetszz/cve/blob/main/upload.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
byzoro -- smart_s85f_firmware	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20231012. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /importexport.php. The manipulation leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243061 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-21	9.8	CVE-2023-5684 MISC <https://github.com/chef003/cve/blob/main/rce.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
calibre-ebook -- calibre	link_to_local_path in ebooks/conversion/plugins/html_input.py in calibre before 6.19.0 can, by default, add resources outside of the document root.	2023-10-22	7.5	CVE-2023-46303 MISC <https://github.com/0x1717/ssrf-via-img> MISC <https://github.com/kovidgoyal/calibre/compare/v6.18.1...v6.19.0>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability was found in CodeAstro Internet Banking System 1.0 and classified as critical. This issue affects some unknown processing of the file pages_reset_pwd.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243131.	2023-10-22	9.8	CVE-2023-5693 MISC MISC MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%201.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
color -- demoiccmax	In International Color Consortium DemoIccMAX 79ecb74, there is a stack-based buffer overflow in the icFixXml function in IccXML/IccLibXML/IccUtilXml.cpp in libIccXML.a.	2023-10-23	8.8	CVE-2023-46602 MISC <https://github.com/internationalcolorconsortium/demoiccmax/pull/53>
color -- demoiccmax	In International Color Consortium DemoIccMAX 79ecb74, there is an out-of-bounds read in the CIccPRMG::GetChroma function in IccProfLib/IccPrmg.cpp in libSampleICC.a.	2023-10-23	7.8	CVE-2023-46603 MISC <https://github.com/internationalcolorconsortium/demoiccmax/pull/53>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- unity_operating_environment	Dell Unity prior to 5.3 contains a Restricted Shell Bypass vulnerability. This could allow an authenticated, local attacker to exploit this vulnerability by authenticating to the device CLI and issuing certain commands.	2023-10-23	7.8	CVE-2023-43066 MISC <https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- unity_operating_environment	Dell Unity 5.3 contain(s) an Arbitrary File Creation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by crafting arbitrary files through a request to the server.	2023-10-23	7.5	CVE-2023-43074 MISC <https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities>
edm_informatics -- e-invoice	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in EDM Informatics E-invoice allows Account Footprinting. This issue affects E-invoice: before 2.1.	2023-10-27	7.5	CVE-2023-5443 MISC <https://www.usom.gov.tr/bildirim/tr-23-0610>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
f5 -- big-ip	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2023-10-26	9.8	CVE-2023-46747 MISC <https://my.f5.com/manage/s/article/k000137353>
f5 -- big-ip	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2023-10-26	8.8	CVE-2023-46748 MISC <https://my.f5.com/manage/s/article/k000137365>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frostming -- pdm	pdm is a Python package and dependency manager supporting the latest PEP standards. It's possible to craft a malicious `pdm.lock` file that could allow e.g., an insider or a malicious open source project to appear to depend on a trusted PyPI project, but actually install another project. A project `foo` can be targeted by creating the project `foo-2` and uploading the file `foo-2-2.tar.gz` to pypi.org. PyPI will see this as project `foo-2` version `2`, while PDM will see this as project `foo` version `2-2`. The version must only be `parseable as a version` and the filename must be a prefix of the project name, but it's not verified to match the version being installed. Version `2-2` is also not a valid normalized version per PEP 440. Matching the project name exactly (not just prefix) would fix the issue. When installing dependencies with PDM, what's actually installed could differ from what's listed in `pyproject.toml` (including arbitrary code execution on install). It could also be used for downgrade attacks by only	2023-10-20	7.8	CVE-2023-45805 MISC <https://github.com/pdm-project/pdm/commit/6853e2642dfa281d4a9958fbc6c95b7e32d84831> MISC <https://github.com/frostming/unearth/blob/eca170d9370ac5032f2e497ee9b1b63823d3fe0f/src/unearth/evaluator.py#l215-l229> MISC <https://gi

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	changing the version. This issue has been addressed in commit `6853e2642df` which is included in release version `2.9.4`. Users are advised to upgrade. There are no known workarounds for this vulnerability.			thub.com/pdm-project/pdm/security/advisories/ghsa-j44v-mmf2-xvm9> MISC <https://github.com/pdm-project/pdm/blob/45d1dfa47d4900c14a31b9bb761e4c46eb5c9442/src/pdm/models/candidates.py#l98-l99> MISC <https://peps.python.org/pep-0440/#post-release-spelling>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_dashboards_on_cloud_pak_for_data	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in container images which could lead to further attacks against the system. IBM X-Force ID: 260730.	2023-10-22	7.5	CVE-2023-38275 MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/260735> MISC <https://www.ibm.com/support/pages/node/7031207>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_dashboards_on_cloud_pak_for_data	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in environment variables which could aid in further attacks against the system. IBM X-Force ID: 260736.	2023-10-22	7.5	CVE-2023-38276 MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/260736> MISC <https://www.ibm.com/support/pages/node/7031207>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_governance	IBM Security Verify Governance 10.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 225222.	2023-10-23	9.8	CVE-2022-22466 MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/225222> MISC <https://www.ibm.com/support/pages/node/7057377>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_governance	IBM Security Verify Governance 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 256036.	2023-10-23	8.8	CVE-2023-33839 MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/256036> MISC <https://www.ibm.com/support/pages/node/7057377>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_governance	IBM Security Verify Governance 10.0 does not encrypt sensitive or critical information before storage or transmission. IBM X-Force ID: 256020.	2023-10-23	7.5	CVE-2023-33837 MISC <https://www.ibm.com/support/pages/node/7057377> MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/256020>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- sterling_partner_engagement_manager	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 could allow a remote user to perform unauthorized actions due to improper authentication. IBM X-Force ID: 266896.	2023-10-23	7.5	CVE-2023-43045 MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/266896> MISC <https://www.ibm.com/support/pages/node/7057409>
idattend -- idweb	Unauthenticated SQL injection in the GetStudentGroupStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26568 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26568>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Unauthenticated SQL injection in the StudentPopupDetails_Timetable method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26569 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26569>
idattend -- idweb	Unauthenticated SQL injection in the GetExcursionList method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26572 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26572>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the SetDB method in IDAttend's IDWeb application 3.1.052 and earlier allows denial of service or theft of database login credentials.	2023-10-25	9.1	CVE-2023-26573 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26573>
idattend -- idweb	Unauthenticated SQL injection in the GetVisitors method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26581 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26581>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Unauthenticated SQL injection in the GetExcursionDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26582 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26582>
idattend -- idweb	Unauthenticated SQL injection in the GetCurrentPeriod method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26583 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26583>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Unauthenticated SQL injection in the GetStudentInconsistencies method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-26584 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26584>
idattend -- idweb	Unauthenticated SQL injection in the GetRoomChanges method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-27254 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27254>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Unauthenticated SQL injection in the DeleteRoomChanges method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-27255 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27255>
idattend -- idweb	Unauthenticated SQL injection in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-27260 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27260>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Unauthenticated SQL injection in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	2023-10-25	9.1	CVE-2023-27262 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27260>
idattend -- idweb	Arbitrary file upload to web root in the IDAttend's IDWeb application 3.1.013 allows authenticated attackers to upload dangerous files to web root such as ASP or ASPX, gaining command execution on the affected server.	2023-10-25	8.8	CVE-2023-26578 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26578>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the StudentPopupDetails_Timetable method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-26570 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26570>
idattend -- idweb	Missing authentication in the SetStudentNotes method in IDAttend's IDWeb application 3.1.052 and earlier allows modification of student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-26571 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26571>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the SearchStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-26574 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26574>
idattend -- idweb	Missing authentication in the SearchStudentsStaff method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student and teacher data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-26575 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26575>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the SearchStudentsRFID method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-26576 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26576>
idattend -- idweb	Unauthenticated arbitrary file read in the IDAttend's IDWeb application 3.1.013 allows the retrieval of any file present on the web server by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-26580 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26580>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the GetActiveToiletPasses method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of student information by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-27257 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27257>
idattend -- idweb	Missing authentication in the GetStudentGroupStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of student and teacher data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-27258 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27258>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student and teacher data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-27259 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27259>
idattend -- idweb	Missing authentication in the StudentPopupDetails_ContactDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-27375 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27375>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the StudentPopupDetails_StudentDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-27376 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27376>
idattend -- idweb	Missing authentication in the StudentPopupDetails_EmergencyContactDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers.	2023-10-25	7.5	CVE-2023-27377 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27377>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inohom -- home_manager_gateway	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in Inohom Home Manager Gateway allows Account Footprinting. This issue affects Home Manager Gateway: before v.1.27.12.	2023-10-27	7.5	CVE-2023-5570 MISC <https://www.usom.gov.tr/bildirim/tr-23-0609>
langchain -- langchain	In Langchain through 0.0.155, prompt injection allows execution of arbitrary code against the SQL service provided by the chain.	2023-10-20	9.8	CVE-2023-32785 MISC <https://gist.github.com/rharang/9c58d39db8c01db5b7c888e467c0533f>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
langchain -- langchain	In Langchain through 0.0.155, prompt injection allows an attacker to force the service to retrieve data from an arbitrary URL, essentially providing SSRF and potentially injecting content into downstream tasks.	2023-10-20	7.5	CVE-2023-32786 MISC <https://gist.github.com/rharang/d265f46fc3161b31ac2e81db44d662e1>
m-files -- web_companion	Execution of downloaded content flaw in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution	2023-10-20	7.8	CVE-2023-5523 MISC <https://www.m-files.com/about/trust-center/security-advisories/cve-2023-5523/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
modoboa -- modoboa	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.2.2.	2023-10-20	8.8	CVE-2023-5690 MISC <https://huntr.com/bounties/980c75a5-d978-4b0e-9bcc-2b2682c97e01> MISC <https://github.com/modoboa/modoboa/commit/23e4c25511c66c0548da001236f47e19e3f9e4d9>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mosparo -- mosparo	Cross-Site Request Forgery (CSRF) in GitHub repository mosparo/mosparo prior to 1.0.3.	2023-10-20	8.8	CVE-2023-5687 MISC <https://huntr.com/bounties/33f95510-cdee-460e-8e61-107874962f2d> MISC <https://github.com/mosparo/mosparo/commit/fb3ac528b7548beb802182310967968a21c1354a>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netentsec -- application_security_gateway	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /protocol/iscgwtunnel/uploadiscgwrouteconf.php. The manipulation of the argument GWLinkId leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243138 is the identifier assigned to this vulnerability.	2023-10-23	9.8	CVE-2023-5700 MISC MISC <https://github.com/istlnight/cve/blob/main/ns-asg-sql-uploadiscgwrouteconf.md> MISC
netentsec -- application_security_gateway	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/list_addr_fwresource_ip.php. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243057 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-20	7.2	CVE-2023-5681 MISC MISC MISC <https://github.com/wsecpro/cve1/blob/main/ns-asg-sql-list_addr_fwresource_ip.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openimageio -- openimageio	An issue in OpenImageIO oiio v.2.4.12.0 allows a remote attacker to execute arbitrary code and cause a denial of service via the read_rle_image function of file bifs/unquantize.c	2023-10-23	8.8	CVE-2023-42295 MISC <https://github.com/openimageio/oiio/issues/3947>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pleaser -- pleaser	please (aka pleaser) through 0.5.4 allows privilege escalation through the TIOCSTI and/or TIOCLINUX ioctl. (If both TIOCSTI and TIOCLINUX are disabled, this cannot be exploited.)	2023-10-20	7.8	CVE-2023-46277 MISC <https://gitlab.com/edneville/please/-/merge_requests/69#note_1594254575> MISC <https://gitlab.com/edneville/please/-/issues/13> MISC <https://rustsec.org/advisories/rustsec-2023-0066.html> MISC <https://github.com/rustsec/advisory-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				db/pull/1798>
projectworlds_pvt._limited -- leave_management_system_project	Leave Management System Project v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'setcasualleave' parameter of the admin/setleaves.php resource does not validate the characters received and they are sent unfiltered to the database.	2023-10-27	9.8	CVE-2023-44480 MISC <https://projectworlds.in/> MISC <https://fluidattacks.com/advisories/martin/>
qnap -- qusbcam2	An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later	2023-10-20	8.8	CVE-2023-23373 MISC <https://www.qnap.com/en/security-advisory/qsa-23-43>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
radare -- radare2	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.9.0.	2023-10-20	8.8	CVE-2023-5686 MISC <https://huntr.com/bounties/bbfe1f76-8fa1-4a8c-909d-65b16e970be0> MISC <https://github.com/radareorg/radare2/commit/1bdda93e348c160c84e30da3637acef26d0348de>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
reconftw -- reconftw	reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities. A vulnerability has been identified in reconftw where inadequate validation of retrieved subdomains may lead to a Remote Code Execution (RCE) attack. An attacker can exploit this vulnerability by crafting a malicious CSP entry on it's own domain. Successful exploitation can lead to the execution of arbitrary code within the context of the application, potentially compromising the system. This issue has been addressed in version 2.7.1.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-10-20	8.8	CVE-2023-46117 MISC <https://github.com/six2dez/reconftw/commit/e639de356c0880fe5fe01a32de9d0c58afb5f086> MISC <https://github.com/six2dez/reconftw/security/advisories/ghsa-fxwr-vr9x-wvjp>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
secudos -- qiata	SECUDOS Qiata (DOMOS OS) 4.13 has Insecure Permissions for the previewRm.sh daily cronjob. To exploit this, an attacker needs access as a low-privileged user to the underlying DOMOS system. Every user on the system has write permission for previewRm.sh, which is executed by the root user.	2023-10-20	7.8	CVE-2023-40361 MISC <https://github.com/vianic/cve-2023-40361/blob/main/advisory/advisory.md>
silabs -- gecko_bootloader	An integer overflow in Silicon Labs Gecko Bootloader version 4.3.1 and earlier allows unbounded memory access when reading from or writing to storage slots.	2023-10-20	7.8	CVE-2023-3487 MISC <https://community.silabs.com/s/contentdocument/0698y00000zmxqlqav> MISC <https://github.com/siliconlabs/gecko_sdk/releases>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sitolog -- sitolog_application_connect	Sitolog sitologapplicationconnect v7.8.a and before was discovered to contain a SQL injection vulnerability via the component /activate_hook.php.	2023-10-20	9.8	CVE-2023-37824 MISC <https://security.friendsofpresta.org/modules/2023/10/11/sitologapplicationconnect.html>
sollace -- unicopia	Sollace Unicopia version 1.1.1 and before was discovered to deserialize untrusted data, allowing attackers to execute arbitrary code.	2023-10-20	9.8	CVE-2023-39680 MISC <https://gist.github.com/apple502j/4ab77291c98e45f4a5bf780c8eda8afa>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	stb_image is a single file MIT licensed library for processing images. It may look like `stbi__load_gif_main` doesn't give guarantees about the content of output value `*delays` upon failure. Although it sets `*delays` to zero at the beginning, it doesn't do it in case the image is not recognized as GIF and a call to `stbi__load_gif_main_outofmem` only frees possibly allocated memory in `*delays` without resetting it to zero. It would be fair to say the caller of `stbi__load_gif_main` is responsible to free the allocated memory in `*delays` only if `stbi__load_gif_main` returns a non-null value. However, at the same time the function may return null value but fail to free the memory in `*delays` if internally `stbi__convert_format` is called and fails. The issue may lead to a memory leak if the caller chooses to free `delays` only when `stbi__load_gif_main` didn't fail or to a double-free if the `delays` is always freed	2023-10-21	9.8	CVE-2023-45666 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l6962-l7045> MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/> MISC <https://github.com/nothings/stb/blob/5

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l6957>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	stb_image is a single file MIT licensed library for processing images. A crafted image file can trigger `stbi__load_gif_main_outofmem` attempt to double-free the out variable. This happens in `stbi__load_gif_main` because when the `layers * stride` value is zero the behavior is implementation defined, but common that realloc frees the old memory and returns null pointer. Since it attempts to double-free the memory a few lines below the first "free", the issue can be potentially exploited only in a multi-threaded environment. In the worst case this may lead to code execution.	2023-10-21	8.8	CVE-2023-45664 MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l6993-l6995>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	stb_image is a single file MIT licensed library for processing images. When `stbi_set_flip_vertically_on_load` is set to `TRUE` and `req_comp` is set to a number that doesn't match the real number of components per pixel, the library attempts to flip the image vertically. A crafted image file can trigger `memcpy` out-of-bounds read because `bytes_per_pixel` used to calculate `bytes_per_row` doesn't match the real image array dimensions.	2023-10-21	8.1	CVE-2023-45662 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l1235> MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	stb_image is a single file MIT licensed library for processing images. If `stbi__load_gif_main` in `stbi_load_gif_from_memory` fails, it returns a null pointer and may keep the `z` variable uninitialized. In case the caller also sets the flip vertically flag, it continues and calls `stbi__vertical_flip_slices` with the null pointer result value and the uninitialized `z` value. This may result in a program crash.	2023-10-21	7.5	CVE-2023-45667 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l1442-l1454> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l1448> MISC <https://securitylab.github.co

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				m/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	stb_image is a single file MIT licensed library for processing images. A crafted image file may trigger out of bounds memcpy read in `stbi__gif_load_next`. This happens because two_back points to a memory address lower than the start of the buffer out. This issue may be used to leak internal memory allocation information.	2023-10-21	7.1	CVE-2023-45661 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l6817> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l7021-l7022> MISC <https://securitylab.github.co

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				m/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[i] = get8_packet(f);`. The root cause is an integer overflow in `setup_malloc`. A sufficiently large value in the variable `sz` overflows with `sz+7` in and the negative value passes the maximum available memory buffer check. This issue may lead to code execution.	2023-10-21	7.8	CVE-2023-45676 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3656> MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/> MISC <https://github.com/nothings/stb/blob/5736b15f7

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l950-l960>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[len] = (char)'\0';`. The root cause is that if `len` read in `start_decoder` is a negative number and `setup_malloc` successfully allocates memory in that case, but memory write is done with a negative index `len`. Similarly if len is INT_MAX the integer overflow len+1 happens in `f->vendor = (char*)setup_malloc(f, sizeof(char) * (len+1));` and `f->comment_list[i] = (char*)setup_malloc(f, sizeof(char) * (len+1));`. This issue may lead to code execution.	2023-10-21	7.8	CVE-2023-45677 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3652-l3658> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3658> MISC <https://securitylab.github.co

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				m/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3653> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3670c7-l3670c75

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l950-l961>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of buffer write in `start_decoder` because at maximum `m->submaps` can be 16 but `submap_floor` and `submap_residue` are declared as arrays of 15 elements. This issue may lead to code execution.	2023-10-21	7.8	CVE-2023-45678 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l4074-l4079> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l753-l760> MISC <https://securitylab

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory allocation failure in `start_decoder`. In that case the function returns early, but some of the pointers in `f->comment_list` are left initialized and later `setup_free` is called on these pointers in `vorbis_deinit`. This issue may lead to code execution.	2023-10-21	7.8	CVE-2023-45679 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3660-l3677> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l4208-l4215> MISC <https://securitylab

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory write past an allocated heap buffer in `start_decoder`. The root cause is a potential integer overflow in `sizeof(char*) * (f->comment_list_length)` which may make `setup_malloc` allocate less memory than required. Since there is another integer overflow an attacker may overflow it too to force `setup_malloc` to return 0 and make the exploit more reliable. This issue may lead to code execution.	2023-10-21	7.8	CVE-2023-45681 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3660-l3677> MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds read in `DECODE` macro when `var` is negative. As it can be seen in the definition of `DECODE_RAW` a negative `var` is a valid value. This issue may be used to leak internal memory allocation information.	2023-10-21	7.1	CVE-2023-45682 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l1717-l1729> MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/> MISC <https://github.com/nothings/stb/blob/5

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l1754-l1756> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3231>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[len] = (char)'\0';`. The root cause is that if the len read in `start_decoder` is `-1` and `len + 1` becomes 0 when passed to `setup_malloc`. The `setup_malloc` behaves differently when `f->alloc.alloc_buffer` is pre-allocated. Instead of returning `NULL` as in `malloc` case it shifts the pre-allocated buffer by zero and returns the currently available memory block. This issue may lead to code execution.	2023-10-21	7.8	CVE-2023-45675 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3652-l3658> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3658> MISC <https://securitylab.github.co

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				m/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l950-l960>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
superwebmailer -- superwebmailer	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows Export SQL Injection via the size parameter.	2023-10-21	8.8	CVE-2023-38190 MISC <https://herolab.usd.de/security-advisories/usd-2023-0014/> MISC <https://herolab.usd.de/security-advisories/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
superwebmailer -- superwebmailer	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows Remote Code Execution via a crafted sendmail command line.	2023-10-21	8.8	CVE-2023-38193 MISC <https://herolab.usd.de/en/security-advisories/usd-2023-0015/> MISC <https://herolab.usd.de/security-advisories/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
thingnario -- photon	An issue in ThingNario Photon v.1.0 allows a remote attacker to execute arbitrary code and escalate privileges via a crafted script to the ping function to the "thingnario Logger Maintenance Webpage" endpoint.	2023-10-21	8.8	CVE-2023-46055 MISC <https://gist.github.com/groundctl2majortom/eef0d55f5df77cc911d84392acdbf625>
tongda -- oa	A vulnerability has been found in Tongda OA 2017 and classified as critical. This vulnerability affects unknown code of the file general/hr/training/record/delete.php. The manipulation of the argument RECORD_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-243058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-20	9.8	CVE-2023-5682 MISC <https://github.com/godfather-onec/cve/blob/main/sql.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- a3700r_firmware	An issue in TOTOLINK A3700R v.9.1.2u.6165_20211012 allows a remote attacker to execute arbitrary code via the FileName parameter of the UploadFirmwareFile function.	2023-10-25	9.8	CVE-2023-46574 MISC <https://github.com/oraclepi/repo/blob/main/totolink%20a3700r/1/a3700r%20%20v9.1.2u.6165_20211012%20vuln.md>
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMapDel.	2023-10-25	9.8	CVE-2023-46554 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/20/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formPortFw.	2023-10-25	9.8	CVE-2023-46555 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/3/1.md> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formFilter.	2023-10-25	9.8	CVE-2023-46556 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/4/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMultiAPVLAN.	2023-10-25	9.8	CVE-2023-46557 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/22/1.md> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMapDelDevice.	2023-10-25	9.8	CVE-2023-46558 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/25/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formIPv6Addr.	2023-10-25	9.8	CVE-2023-46559 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/9/1.md>
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formTcpipSetup.	2023-10-25	9.8	CVE-2023-46560 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/23/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formDosCfg.	2023-10-25	9.8	CVE-2023-46562 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/8/1.md>
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formIpQoS.	2023-10-25	9.8	CVE-2023-46563 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/7/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formDMZ.	2023-10-25	9.8	CVE-2023-46564 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/6/1.md> MISC
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function uninstallPluginReqHandle.	2023-10-25	9.8	CVE-2023-46520 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/1/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function RegisterRegister.	2023-10-25	9.8	CVE-2023-46521 MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/11/1.md> MISC
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function deviceInfoRegister.	2023-10-25	9.8	CVE-2023-46522 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/2/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function upgradeInfoRegister.	2023-10-25	9.8	CVE-2023-46523 MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/3/1.md> MISC
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function loginRegister.	2023-10-25	9.8	CVE-2023-46525 MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/12/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function resetCloudPwdRegister.	2023-10-25	9.8	CVE-2023-46526 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/10/1.md>
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function bindRequestHandle.	2023-10-25	9.8	CVE-2023-46527 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/13/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function modifyAccPwdRegister.	2023-10-25	9.8	CVE-2023-46534 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/9/1.md>
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getResetVeriRegister.	2023-10-25	9.8	CVE-2023-46535 MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/6/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkRegVeriRegister.	2023-10-25	9.8	CVE-2023-46536 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/5/1.md>
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getRegVeriRegister.	2023-10-25	9.8	CVE-2023-46537 MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/7/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkResetVeriRegister.	2023-10-25	9.8	CVE-2023-46538 MISC MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/4/1.md>
tp-link -- tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function registerRequestHandle.	2023-10-25	9.8	CVE-2023-46539 MISC <https://github.com/xyiym/digging/blob/main/tp-link/tl-wr886n/8/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trtek_software -- education_portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TRtek Software Education Portal allows SQL Injection. This issue affects Education Portal: before 3.2023.29.	2023-10-27	9.8	CVE-2023-5807 MISC <https://www.usom.gov.tr/bildirim/tr-23-0608>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vercel -- next.js	Next.js before 13.4.20-canary.13 lacks a cache-control header and thus empty prefetch responses may sometimes be cached by a CDN, causing a denial of service to all users requesting the same URL via that CDN.	2023-10-22	7.5	CVE-2023-46298 MISC <https://github.com/vercel/next.js/issues/45301> MISC <https://github.com/vercel/next.js/compare/v13.4.20-canary.12...v13.4.20-canary.13> MISC <https://github.com/vercel/next.js/pull/54732>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware -- fusion	VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time.	2023-10-20	7.8	CVE-2023-34045 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0022.html>
vmware -- fusion	VMware Fusion(13.x prior to 13.5) contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time.	2023-10-20	7	CVE-2023-34046 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0022.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wallix -- bastion	WALLIX Bastion 9.x before 9.0.9 and 10.x before 10.0.5 allows unauthenticated access to sensitive information by bypassing access control on a network access administration web interface.	2023-10-23	7.5	CVE-2023-46319 MISC <https://www.wallix.com/support/alerts/>
wordpress -- wordpress	The Ad Inserter for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.7.30 via the ai-debug-processing-fe URL parameter. This can allow unauthenticated attackers to extract sensitive data including installed plugins (present and active), active theme, various plugin settings, WordPress version, as well as some server settings such as memory limit, installation paths.	2023-10-20	7.5	CVE-2023-4668 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Jetpack CRM plugin for WordPress is vulnerable to PHAR deserialization via the 'zbscrmcsvimpf' parameter in the 'zeroBSCRM_CSVImporterLitehtml_app' function in versions up to, and including, 5.3.1. While the function performs a nonce check, steps 2 and 3 of the check do not take any action upon a failed check. These steps then perform a 'file_exists' check on the value of 'zbscrmcsvimpf'. If a phar:// archive is supplied, its contents will be deserialized and an object injected in the execution stream. This allows an unauthenticated attacker to obtain object injection if they are able to upload a phar archive (for instance if the site supports image uploads) and then trick an administrator into performing an action, such as clicking a link.	2023-10-20	8.8	CVE-2022-3342 MISC <https://plugins.trac.wordpress.org/changeset/2805282/zero-bs-crm/trunk/includes/zerobscrm.csvimporter.php> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Brizy plugin for WordPress is vulnerable to authorization bypass due to an incorrect capability check on the is_administrator() function in versions up to, and including, 1.0.125. This makes it possible for authenticated attackers to access and interact with available AJAX functions.	2023-10-20	8.1	CVE-2020-36714 MISC MISC <https://blog.nintechnet.com/wordpress-brizy-page-builder-plugin-fixed-critical-vulnerabilities/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Security & Malware scan by CleanTalk plugin for WordPress is vulnerable to unauthorized user interaction in versions up to, and including, 2.50. This is due to missing capability checks on several AJAX actions and nonce disclosure in the source page of the administrative dashboard. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to call functions and delete and/or upload files.	2023-10-20	8.8	CVE-2020-36698 MISC <https://blog.nintechnet.com/multiple-vulnerabilities-fixed-in-security-malware-scan-by-cleantalk-plugin/> MISC <https://wpscan.com/vulnerability/23960f42-dfc1-4951-9169-02d889283f01> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Cyr to Lat plugin for WordPress is vulnerable to authenticated SQL Injection via the 'ctl_sanitize_title' function in versions up to, and including, 3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This potentially allows authenticated users with the ability to add or modify terms or tags to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. A partial patch became available in version 3.6 and the issue was fully patched in version 3.7.	2023-10-20	8.8	CVE-2022-4290 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Horizontal scrolling announcement plugin for WordPress is vulnerable to SQL Injection via the plugin's [horizontal-scrolling] shortcode in versions up to, and including, 9.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2023-10-20	8.8	CVE-2023-4999 MISC MISC <https://plugins.trac.wordpress.org/browser/horizontal-scrolling-announcement/trunk/horizontal-scrolling-announcement.php#l79>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Dropbox Folder Share for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 1.9.7 via the editor-view.php file. This allows unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2023-10-20	9.8	CVE-2023-4488 MISC MISC
wordpress -- wordpress	The Icegram Express plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 5.6.23 via the show_es_logs function. This allows administrator-level attackers to read the contents of arbitrary files on the server, which can contain sensitive information including those belonging to other sites, for example in shared hosting environments.	2023-10-20	7.2	CVE-2023-5414 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The ImageMagick Engine plugin for WordPress is vulnerable to remote code execution via the 'cli_path' parameter in versions up to and including 1.7.5. This makes it possible for unauthenticated users to run arbitrary commands leading to remote command execution, granted they can trick a site administrator into performing an action such as clicking on a link. This makes it possible for an attacker to create and or modify files hosted on the server which can easily grant attackers backdoor access to the affected server.	2023-10-20	8.8	CVE-2022-2441 MISC <https://github.com/orangelabweb/imagemagick-engine/blob/v.1.7.2/imagemagick-engine.php#l529> MISC <https://www.exploit-db.com/exploits/51025> MISC <https://github.com/orangelabweb/imagemagick-engine/blob/1.7.4/imagemagick-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				engine.php#l529> MISC <https://www.wordfence.com/vulnerability-advisories-continued/#cve-2022-2441> MISC MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in PluginEver WC Serial Numbers plugin <= 1.6.3 versions.	2023-10-21	8.8	CVE-2023-46078 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_save_options function. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Additionally, input sanitization and escaping is insufficient resulting in the possibility of malicious script injection.	2023-10-20	8.8	CVE-2023-4920 MISC MISC MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/index.php#l805>
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Qwerty23 Rocket Font plugin <= 1.2.3 versions.	2023-10-21	8.8	CVE-2023-46067 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Fancy Product Designer plugin for WordPress is vulnerable to unauthorized modification of site options due to a missing capability check on the fpd_update_options function in versions up to, and including, 4.6.9. This makes it possible for authenticated attackers with subscriber-level permissions to modify site options, including setting the default role to administrator which can allow privilege escalation.	2023-10-20	8.8	CVE-2021-4334 MISC MISC <https://support.fancyproductdesigner.com/support/discussions/topics/13000029981>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Simple:Press - WordPress Forum Plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ~/admin/resources/jscript/ajaxupload/sf-uploader.php file in versions up to, and including, 6.6.0. This makes it possible for attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	2023-10-20	9.8	CVE-2020-36706 MISC MISC <https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-simple-press-wordpress-forum-arbitrary-file-upload-6-6-0/> MISC <https://blog.nintechnet.com/wordpress-simplepress-plugin-fixed-critical-vulnerabilities/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://wpscan.com/vulnerability/27d4a8a5-9d81-4b42-92be-3f7d1ef22843>
wordpress -- wordpress	The Soisy Pagamento Rateale plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the parseRemoteRequest function in versions up to, and including, 6.0.1. This makes it possible for unauthenticated attackers with knowledge of an existing WooCommerce Order ID to expose sensitive WooCommerce order information (e.g., Name, Address, Email Address, and other order metadata).	2023-10-21	7.5	CVE-2023-5132 MISC MISC <https://plugins.trac.wordpress.org/browser/soisy-pagamento-rateale/trunk/public/class-soisy-pagamento-rateale-public.php#l465>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_posts function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2023-10-20	8.1	CVE-2023-4386 MISC MISC
wordpress -- wordpress	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_products function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2023-10-20	9.8	CVE-2023-4402 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 0.9.91 via Google Drive API secrets stored in plaintext in the publicly visible plugin source. This could allow unauthenticated attackers to impersonate the WPVivid Google Drive account via the API if they can trick a user into reauthenticating via another vulnerability or social engineering.	2023-10-20	9.3	CVE-2023-5576 MISC <https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/tags/0.9.91/includes/customclass/client_secrets.json> MISC MISC <https://plugins.trac.wordpress.org/changeset/2977863/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zscaler -- client_connector	An Improper Input Validation vulnerability in Zscaler Client Connector on Linux allows Privilege Escalation. This issue affects Client Connector: before 1.4.0.105	2023-10-23	9.8	CVE-2023-28805 MISC <https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023>
zscaler -- client_connector	The Zscaler Client Connector Installer and Unsintallers for Windows prior to 3.6 had an unquoted search path vulnerability. A local adversary may be able to execute code with SYSTEM privileges.	2023-10-23	7.8	CVE-2021-26735 MISC <https://help.zscaler.com/zscaler-client-connector/client-connector-app-release-summary-2021>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zscaler -- client_connector	Multiple vulnerabilities in the Zscaler Client Connector Installer and Uninstaller for Windows prior to 3.6 allowed execution of binaries from a low privileged path. A local adversary may be able to execute code with SYSTEM privileges.	2023-10-23	7.8	CVE-2021-26736 MISC <https://help.zscaler.com/zscaler-client-connector/client-connector-app-release-summary-2021>
zscaler -- client_connector	Zscaler Client Connector for macOS prior to 3.7 had an unquoted search path vulnerability via the PATH variable. A local adversary may be able to execute code with root privileges.	2023-10-23	7.8	CVE-2021-26738 MISC
zscaler -- client_connector	Buffer overflow vulnerability in the signelf library used by Zscaler Client Connector on Linux allows Code Injection. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	2023-10-23	7.8	CVE-2023-28793 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zscaler -- client_connector	Origin Validation Error vulnerability in Zscaler Client Connector on Linux allows Inclusion of Code in Existing Process. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	2023-10-23	7.8	CVE-2023-28795 MISC
zscaler -- client_connector	Improper Verification of Cryptographic Signature vulnerability in Zscaler Client Connector on Linux allows Code Injection. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	2023-10-23	7.8	CVE-2023-28796 MISC
zscaler -- client_connector	Zscaler Client Connector for Windows before 4.1 writes/deletes a configuration file inside specific folders on the disk. A malicious user can replace the folder and execute code as a privileged user.	2023-10-23	7.3	CVE-2023-28797 MISC <https://help.zscaler.com/client-connector/client-connector-app-release-summary-2022>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zzzcms -- zzzcms	File Upload vulnerability in zzzCMS v.2.1.9 allows a remote attacker to execute arbitrary code via modification of the imageext parameter from jpg, jpeg,gif, and png to jpg, jpeg,gif, png, pphphp.	2023-10-25	9.8	CVE-2023-45554 MISC <https://github.com/96xiaopang/vulnerabilities/blob/main/zzzcms%e4%bb%bb%e6%84%8f%e6%96%87%e4%bb%b6%e4%b8%8a%e4%bc%a0_en.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zzzcms -- zzzcms	File Upload vulnerability in zzzCMS v.2.1.9 allows a remote attacker to execute arbitrary code via a crafted file to the down_url function in zzz.php file.	2023-10-25	7.8	CVE-2023-45555 MISC <https://github.com/96xiaopang/vulnerabilities/blob/main/zzzcms%e4%bb%bb%e6%84%8f%e6%96%87%e4%bb%b6%e4%b8%8a%e4%bc%a0_en.md>

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- airflow	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Airflow.This issue affects Apache Airflow from 2.4.0 to 2.7.0. Sensitive configuration information has been exposed to authenticated users with the ability to read configuration via Airflow REST API for configuration even when the expose_config option is set to non-sensitive-only. The expose_config option is False by default. It is recommended to upgrade to a version that is not affected if you set expose_config to non-sensitive-only configuration. This is a different error than CVE-2023-45348 which allows authenticated user to retrieve individual configuration values in 2.7.* by specially crafting their request (solved in 2.7.2). Users are recommended to upgrade to version 2.7.2, which fixes the issue and additionally fixes CVE-2023-45348.	2023-10-23	4.3	CVE-2023-46288 MISC <https://github.com/apache/airflow/pull/32261> MISC <https://lists.apache.org/thread/yw4vzm0c5lqkwm0bxv6qy03yfd1od4nw>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- santuario_xml_security_for_java	All versions of Apache Santuario - XML Security for Java prior to 2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is enabled. Users are recommended to upgrade to version 2.2.6, 2.3.4, or 3.0.3, which fixes this issue.	2023-10-20	6.5	CVE-2023-44483 MISC <https://lists.apache.org/thread/vmqbp9mfxtrf0kmbnnmbn3h9j6dr9q55> MISC <http://www.openwall.com/lists/oss-security/2023/10/20/5>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the extra parameter in the news menu component.	2023-10-20	5.4	CVE-2023-43353 MISC <https://github.com/sromanhu/cve-2023-43353-cmsmadesimple-stored-xss---news---extra>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Profiles parameter in the Extensions -MicroTiny WYSIWYG editor component.	2023-10-20	5.4	CVE-2023-43354 MISC <https://github.com/sromanhu/cve-2023-43354-cmsmadesimple-stored-xss---microtiny-extension>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the password and password again parameters in the My Preferences - Add user component.	2023-10-20	5.4	CVE-2023-43355 MISC <https://github.com/sromanhu/cve-2023-43355-cmsmadesimple-reflected-xss---add-user> MISC <https://github.com/sromanhu/cmsmadesimple-reflected-xss---add-user>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Global Meatadata parameter in the Global Settings Menu component.	2023-10-20	5.4	CVE-2023-43356 MISC <https://github.com/sromanhu/cve-2023-43356-cmsmadesimple-stored-xss---global-settings>
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Title parameter in the Manage Shortcuts component.	2023-10-20	5.4	CVE-2023-43357 MISC <https://github.com/sromanhu/cve-2023-43357-cmsmadesimple-stored-xss---shortcut>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been classified as problematic. Affected is an unknown function of the file pages_system_settings.php. The manipulation of the argument sys_name with the input <ScRiPt >alert(991)</ScRiPt> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243132.	2023-10-22	6.1	CVE-2023-5694 MISC MISC MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%202.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file pages_reset_pwd.php. The manipulation of the argument email with the input testing%40example.com'%26%25<ScRiPt%20>alert(9860)</ScRiPt> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243133 was assigned to this vulnerability.	2023-10-22	6.1	CVE-2023-5695 MISC MISC MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%203.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file pages_transfer_money.php. The manipulation of the argument account_number with the input 357146928--><ScRiPt%20>alert(9206)</ScRiPt><!--leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-243134 is the identifier assigned to this vulnerability.	2023-10-22	6.1	CVE-2023-5696 MISC MISC MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%204.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability classified as problematic has been found in CodeAstro Internet Banking System 1.0. This affects an unknown part of the file pages_withdraw_money.php. The manipulation of the argument account_number with the input 287359614--><ScRiPt%20>alert(1234)</ScRiPt><!--leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243135.	2023-10-23	6.1	CVE-2023-5697 MISC MISC MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%205.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. This vulnerability affects unknown code of the file pages_deposit_money.php. The manipulation of the argument account_number with the input 421873905--><ScRiPt%20>alert(9523)</ScRiPt><!--leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243136.	2023-10-23	6.1	CVE-2023-5698 MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%206.pdf> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- internet_banking_system	A vulnerability, which was classified as problematic, has been found in CodeAstro Internet Banking System 1.0. This issue affects some unknown processing of the file pages_view_client.php. The manipulation of the argument acc_name with the input Johnnie Reyes'"()&%<zzz><ScRiPt >alert(5646)</ScRiPt> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243137 was assigned to this vulnerability.	2023-10-23	6.1	CVE-2023-5699 MISC MISC MISC <https://github.com/e1cho/cve_hub/blob/main/internet%20banking%20system/internet%20banking%20system%20-%20vuln%207.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- unity_operating_environment	Dell Unity prior to 5.3 contains an XML External Entity injection vulnerability. An XXE attack could potentially exploit this vulnerability disclosing local files in the file system.	2023-10-23	6.5	CVE-2023-43067 MISC <https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- unity_operating_environment	Dell Unity prior to 5.3 contains a Cross-site scripting vulnerability. A low-privileged authenticated attacker can exploit these issues to obtain escalated privileges.	2023-10-23	5.4	CVE-2023-43065 MISC <https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
enhancesoft -- osticket	A stored cross-site scripting (XSS) vulnerability in the Admin panel in Enhancesoft osTicket v1.17.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Role Name parameter.	2023-10-23	4.8	CVE-2023-27148 MISC <https://www.esecforte.com/cve-2023-27148-osticket_xss/>
enhancesoft -- osticket	A stored cross-site scripting (XSS) vulnerability in Enhancesoft osTicket v1.17.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Label input parameter when updating a custom list.	2023-10-23	4.8	CVE-2023-27149 MISC <https://www.esecforte.com/cve-2023-27149-osticket_xss/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
home-assistant -- home-assistant	Home assistant is an open source home automation. The audit team's analyses confirmed that the `redirect_uri` and `client_id` are alterable when logging in. Consequently, the code parameter utilized to fetch the `access_token` post-authentication will be sent to the URL specified in the aforementioned parameters. Since an arbitrary URL is permitted and `homeassistant.local` represents the preferred, default domain likely used and trusted by many users, an attacker could leverage this weakness to manipulate a user and retrieve account access. Notably, this attack strategy is plausible if the victim has exposed their Home Assistant to the Internet, since after acquiring the victim's `access_token` the adversary would need to utilize it directly towards the instance to achieve any pertinent malicious actions. To achieve this compromise attempt, the attacker must send a link with a `redirect_uri` that they control to the victim's own Home Assistant	2023-10-20	5.4	CVE-2023-41893 MISC <https://www.home-assistant.io/blog/2023/10/19/security-audits-of-home-assistant/> MISC <https://github.com/home-assistant/core/security/advisories/ghsa-qhhj-7hrc-gqj5>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	instance. In the eventuality the victim authenticates via said link, the attacker would obtain code sent to the specified URL in `redirect_uri`, which can then be leveraged to fetch an `access_token`. Pertinently, an attacker could increase the efficacy of this strategy by registering a near identical domain to `homeassistant.local`, which at first glance may appear legitimate and thereby obfuscate any malicious intentions. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
home-assistant -- home-assistant	Home assistant is an open source home automation. The assessment verified that webhooks available in the webhook component are triggerable via the `*.ui.nabu.casa` URL without authentication, even when the webhook is marked as Only accessible from the local network. This issue is facilitated by the SniTun proxy, which sets the source address to 127.0.0.1 on all requests sent to the public URL and forwarded to the local Home Assistant. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-10-20	5.3	CVE-2023-41894 MISC <https://github.com/home-assistant/core/security/advisories/ghsa-wx3j-3v2j-rf45> MISC <https://www.home-assistant.io/blog/2023/10/19/security-audits-of-home-assistant/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
i-doit -- i-doit	I-doit pro 25 and below is vulnerable to Cross Site Scripting (XSS) via index.php.	2023-10-21	5.4	CVE-2023-46003 MISC <https://www.i-doit.com/> MISC <https://medium.com/@ray.999/stored-xss-in-i-doit-pro-25-and-below-cve-2023-46003-17fb8d6fe2e9> MISC <https://github.com/leekenghwa/cve-2023-46003>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_dashboards_on_cloud_pak_for_data	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a victim to a phishing site. IBM X-Force ID: 262482.	2023-10-22	6.5	CVE-2023-38735 MISC <https://www.ibm.com/support/pages/node/7031207> MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/262482>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_governance	IBM Security Verify Governance 10.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256037.	2023-10-23	4.8	CVE-2023-33840 MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/256037> MISC <https://www.ibm.com/support/pages/node/7057377>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- sterling_partner_engagement_manager	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262174.	2023-10-23	5.4	CVE-2023-38722 MISC <https://www.ibm.com/support/pages/node/7057407> MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/262174>
idattend -- idweb	Missing authentication in the DeleteAssignments method in IDAttend's IDWeb application 3.1.052 and earlier allows deletion of data by unauthenticated attackers.	2023-10-25	6.5	CVE-2023-27261 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27261>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Stored cross-site scripting in the IDAttend's IDWeb application 3.1.052 and earlier allows attackers to hijack the browsing session of the logged in user.	2023-10-25	5.4	CVE-2023-26577 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26577>
idattend -- idweb	Missing authentication in the DeleteStaff method in IDAttend's IDWeb application 3.1.013 allows deletion of staff information by unauthenticated attackers.	2023-10-25	5.3	CVE-2023-26579 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-26579>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idattend -- idweb	Missing authentication in the GetLogFiles method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of sensitive log files by unauthenticated attackers.	2023-10-25	5.3	CVE-2023-27256 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-27256>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kaibutsunosato -- kaibutsunosato	The leakage of the client secret in Kaibutsunosato v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-20	5.3	CVE-2023-39731 MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39731.md> MISC <https://liff.line.me/1657662489-pweqnzj4>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
m-files -- classic_web	Stored XSS Vulnerability in M-Files Classic Web versions before 23.10 and LTS Service Release Versions before 23.2 LTS SR4 and 23.8 LTS SR1allows attacker to execute script on users browser via stored HTML document.	2023-10-20	5.4	CVE-2023-2325 MISC <https://www.m-files.com/about/trust-center/security-advisories/cve-2023-2325/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
modoboa -- modoboa	Cross-site Scripting (XSS) - DOM in GitHub repository modoboa/modoboa prior to 2.2.2.	2023-10-20	5.4	CVE-2023-5688 MISC <https://huntr.com/bounties/0ceb10e4-952b-4ca4-baf8-5b6f12e3a8a7> MISC <https://github.com/modoboa/modoboa/commit/d33d3cd2d11dbfebd8162c46e2c2a9873919a967>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
modoboa -- modoboa	Cross-site Scripting (XSS) - DOM in GitHub repository modoboa/modoboa prior to 2.2.2.	2023-10-20	5.4	CVE-2023-5689 MISC <https://github.com/modoboa/modoboa/commit/d33d3cd2d11dbfebd8162c46e2c2a9873919a967> MISC <https://huntr.com/bounties/24835833-3421-412b-bafb-1b7ea3cf60e6>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nagvis -- nagvis	XSS exists in NagVis before 1.9.38 via the select function in share/server/core/functions/html.php.	2023-10-20	6.1	CVE-2023-46287 MISC <https://github.com/nagvis/nagvis/compare/nagvis-1.9.37...nagvis-1.9.38> MISC <https://github.com/nagvis/nagvis/pull/356> MISC <https://github.com/nagvis/nagvis/pull/356/commits/d660591b23e5cfea4d1be2d3fb8f3855aa6020fb>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opensolution -- quick_cms	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the Backend - Dashboard parameter in the Languages Menu component.	2023-10-20	5.4	CVE-2023-43346 MISC <https://github.com/sromanhu/quick-cms-stored-xss---languages-backend> MISC <https://github.com/sromanhu/cve-2023-43346-quick-cms-stored-xss---languages-backend>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	stb_image is a single file MIT licensed library for processing images. The stbi__getn function reads a specified number of bytes from context (typically a file) into the specified buffer. In case the file stream points to the end, it returns zero. There are two places where its return value is not checked: In the `stbi__hdr_load` function and in the `stbi__tga_load` function. The latter of the two is likely more exploitable as an attacker may also control the size of an uninitialized buffer.	2023-10-21	5.5	CVE-2023-45663 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l5936c10-l5936c20> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l7221> MISC <https://gi

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				thub.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#l1664> MISC <https://securitylab.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_vorbis.c -- stb_vorbis.c	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory allocation failure in `start_decoder`. In that case the function returns early, the `f->comment_list` is set to `NULL`, but `f->comment_list_length` is not reset. Later in `vorbis_deinit` it tries to dereference the `NULL` pointer. This issue may lead to denial of service.	2023-10-21	5.5	CVE-2023-45680 MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l3660-l3666> MISC <https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#l4208-l4215> MISC <https://securitylab

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				.github.com/advisories/ghsl-2023-145_ghsl-2023-151_stb_image_h/>
superwebmailer -- superwebmailer	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows spamtest_external.php XSS via a crafted filename.	2023-10-20	6.1	CVE-2023-38191 MISC <https://herolab.usd.de/security-advisories/> MISC <https://herolab.usd.de/security-advisories/usd-2023-0012/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
superwebmailer -- superwebmailer	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows superadmincreate.php XSS via crafted incorrect passwords.	2023-10-21	6.1	CVE-2023-38192 MISC <https://herolab.usd.de/security-advisories/> MISC <https://herolab.usd.de/security-advisories/usd-2023-0011/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
superwebmailer -- superwebmailer	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows keepalive.php XSS via a GET parameter.	2023-10-21	6.1	CVE-2023-38194 MISC <https://herolab.usd.de/security-advisories/> MISC <https://herolab.usd.de/security-advisories/usd-2023-0013/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tauri -- tauri	Tauri is a framework for building binaries for all major desktop platforms. This advisory is not describing a vulnerability in the Tauri code base itself but a commonly used misconfiguration which could lead to leaking of the private key and updater key password into bundled Tauri applications using the Vite frontend in a specific configuration. The Tauri documentation used an insecure example configuration in the `Vite guide` to showcase how to use Tauri together with Vite. Copying the following snippet `envPrefix: ['VITE_', 'TAURI_'],` from this guide into the `vite.config.ts` of a Tauri project leads to bundling the `TAURI_PRIVATE_KEY` and `TAURI_KEY_PASSWORD` into the Vite frontend code and therefore leaking this value to the released Tauri application. Using the `envPrefix: ['VITE_'],` or any other framework than Vite means you are not impacted by this advisory. Users are advised to rotate their updater private key if they are affected by this (requires Tauri CLI >=1.5.5). After updating the	2023-10-20	5.5	CVE-2023-46115 MISC <https://github.com/tauri-apps/tauri/security/advisories/ghsa-2rcp-jvr4-r259> MISC <https://tauri.app/v1/guides/getting-started/setup/vite/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	envPrefix configuration, generate a new private key with `tauri signer generate`, saving the new private key and updating the updater's `pubkey` value on `tauri.conf.json` with the new public key. To update your existing application, the next application build must be signed with the older private key in order to be accepted by the existing application.			
vmware -- workstation	VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine.	2023-10-20	6	CVE-2023-34044 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0022.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vnote_project -- vnote	A vulnerability has been found in vnotex vnote up to 3.17.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Markdown File Handler. The manipulation with the input <xss onclick="alert(1)" style=display:block>Click here</xss> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243139. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-23	6.1	CVE-2023-5701 MISC <https://github.com/victorootnice/victorootnice.github.io/blob/main/2023/bbp-01.md> MISC MISC
wbce -- wbce_cms	Cross Site Scripting (XSS) vulnerability in WBCE CMS v.1.6.1 and before allows a remote attacker to escalate privileges via a crafted script to the website_footer parameter in the admin/settings/save.php component.	2023-10-21	5.4	CVE-2023-46054 MISC <https://github.com/aaanz/aaanz.github.io/blob/master/xss.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Blog2Social plugin for WordPress is vulnerable to authorization bypass due to missing capability checks in versions up to, and including, 6.9.11. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to change some plugin settings intended to be modifiable by admins only.	2023-10-20	4.3	CVE-2022-3622 MISC MISC <https://plugins.trac.wordpress.org/browser/blog2social/tags/6.9.10/includes/b2s/settings/item.php#l116> MISC MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Alex Raven WP Report Post plugin <= 2.1.2 versions.	2023-10-25	6.1	CVE-2023-45769 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Milesi Amministrazione Trasparente plugin <= 8.0.2 versions.	2023-10-25	4.8	CVE-2023-45758 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Add Custom Body Class plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'add_custom_body_class' value in versions up to, and including, 1.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-21	5.4	CVE-2023-5205 MISC MISC <https://plugins.trac.wordpress.org/browser/add-custom-body-class/trunk/add-custom-body-class.php#l32>
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anurag Deshmukh CPT Shortcode Generator plugin <= 1.0 versions.	2023-10-25	4.8	CVE-2023-45644 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Biztechc Copy or Move Comments plugin <= 5.0.4 versions.	2023-10-25	6.1	CVE-2023-45634 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The ARMember Lite - Membership Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 4.0.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2023-10-20	4.8	CVE-2023-3996 MISC <https://www.armemberplugin.com> MISC MISC <https://plugins.svn.wordpress.org/armember-membership/tags/4.0.2/readme.md> MISC MISC <https://plugins.svn.wordpress.org/armember-membership/tags/4.0.2/readme.txt>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Booster for WooCommerce for WordPress is vulnerable to Information Disclosure via the 'wcj_wp_option' shortcode in versions up to, and including, 7.1.0 due to insufficient controls on the information retrievable via the shortcode. This makes it possible for authenticated attackers, with subscriber-level capabilities or above, to retrieve arbitrary sensitive site options.	2023-10-20	4.3	CVE-2023-4796 MISC <https://plugins.trac.wordpress.org/changeset/2966325/woocommerce-jetpack#file1> MISC <https://plugins.trac.wordpress.org/browser/woocommerce-jetpack/tags/7.1.0/includes/shortcodes/class-wcj-general-shortcodes.php#l450> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BuddyBoss BuddyPress Global Search plugin <= 1.2.1 versions.	2023-10-25	4.8	CVE-2023-45755 MISC
wordpress -- wordpress	The WP Cerber Security plugin for WordPress is vulnerable to stored cross-site scripting via the log parameter when logging in to the site in versions up to, and including, 9.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	6.1	CVE-2022-4712 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Woody code snippets plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3.9. This is due to missing or incorrect nonce validation on the runActions() function. This makes it possible for unauthenticated attackers to activate and deactivate snippets via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2020-36759 MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintechnet.com/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/> MISC <https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-5/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Photospace Responsive plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'psres_button_size' parameter in versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2023-10-20	4.8	CVE-2023-4271 MISC MISC MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Fastwpspeed Fast WP Speed plugin <= 1.0.0 versions.	2023-10-25	6.1	CVE-2023-45770 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WhatsApp Share Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'whatsapp' shortcode in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5668 MISC MISC <https://plugins.trac.wordpress.org/browser/whatsapp/tags/1.0.1/class-frontend.php#l46>
wordpress -- wordpress	The flowpaper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'flipbook' shortcode in versions up to, and including, 2.0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5200 MISC MISC <https://plugins.trac.wordpress.org/changeset/2966821/flowpaper-lite-pdf-flipbook> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Scroll post excerpt plugin <= 8.0 versions.	2023-10-25	4.8	CVE-2023-45764 MISC
wordpress -- wordpress	The WP Customer Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 3.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2023-10-20	4.8	CVE-2023-4648 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The wpDiscuz plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the voteOnComment function in versions up to, and including, 7.6.3. This makes it possible for unauthenticated attackers to increase or decrease the rating of a comment.	2023-10-20	5.3	CVE-2023-3869 MISC MISC <https://plugins.trac.wordpress.org/browser/wpdiscuz/trunk/utils/class.wpdiscuzhelperajax.php#l681>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The wpDiscuz plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the userRate function in versions up to, and including, 7.6.3. This makes it possible for unauthenticated attackers to increase or decrease the rating of a post.	2023-10-20	5.3	CVE-2023-3998 MISC <https://plugins.trac.wordpress.org/browser/wpdiscuz/trunk/utils/class.wpdiscuzhelperajax.php#l886> MISC
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in HappyBox Newsletter & Bulk Email Sender - Email Newsletter Plugin for WordPress plugin <= 2.0.1 versions.	2023-10-25	5.4	CVE-2023-45829 MISC
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Henryholtgeerts PDF Block plugin <= 1.1.0 versions.	2023-10-25	5.4	CVE-2023-45646 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Easy Testimonial Slider and Form plugin <= 1.0.18 versions.	2023-10-25	4.8	CVE-2023-45754 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The iframe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `iframe` shortcode in versions up to, and including, 4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permission and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 4.6 and fully patched in version 4.7.	2023-10-20	5.4	CVE-2023-4919 MISC <https://plugins.trac.wordpress.org/browser/iframe/tags/4.5/iframe.php#l40> MISC <https://plugins.trac.wordpress.org/browser/iframe/tags/4.5/iframe.php#l28> MISC MISC <https://plugins.trac.wordpress.org/changeset/2970787/iframe#file4>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WP Mailto Links - Protect Email Addresses plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wpml_mailto' shortcode in versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 3.1.3 and fully patched in version 3.1.4.	2023-10-20	5.4	CVE-2023-5109 MISC MISC <https://plugins.trac.wordpress.org/browser/wp-mailto-links/tags/3.1.2/core/includes/classes/class-wp-mailto-links-validate.php#l582>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Coupon Creator plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.1. This is due to missing or incorrect nonce validation on the save_meta() function. This makes it possible for unauthenticated attackers to save meta fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2020-36751 MISC <https://plugins.trac.wordpress.org/changeset/2368658/coupon-creator/tags/2.5.2.1/plugin-engine/src/pngx/admin/meta.php> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://bl

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				og.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				1/> MISC <https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				vulnerabilities-part-5/>
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Joovii Sendle Shipping Plugin plugin <= 5.13 versions.	2023-10-25	6.1	CVE-2023-45761 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Copy Anything to Clipboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'copy' shortcode in versions up to, and including, 2.6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5086 MISC <https://plugins.trac.wordpress.org/changeset/2969441/copy-the-code#file1> MISC MISC <https://plugins.trac.wordpress.org/browser/copy-the-code/tags/2.6.4/classes/class-copy-the-code-shortcode.php#l83>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in EventPrime EventPrime - Events Calendar, Bookings and Tickets plugin <= 3.1.5 versions.	2023-10-25	6.1	CVE-2023-45637 MISC
wordpress -- wordpress	The Auto Amazon Links plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the style parameter in versions up to, and including, 5.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-4482 MISC MISC
wordpress -- wordpress	The miniOrange's Google Authenticator plugin for WordPress is vulnerable to authorization bypass due to a missing capability check when changing plugin settings in versions up to, and including, 5.6.5. This makes it possible for unauthenticated attackers to change the plugin's settings.	2023-10-20	5.3	CVE-2022-4943 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The EventON plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 2.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2023-10-21	6.1	CVE-2023-4635 MISC MISC <https://github.com/xsn1210/vul/blob/main/xss%5beventon%5d%20.md>
wordpress -- wordpress	The Winters theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.4.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2023-10-20	6.1	CVE-2023-3962 MISC MISC <https://github.com/blackfan/client-side-prototype-pollution>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Paid Memberships Pro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4.2. This is due to missing or incorrect nonce validation on the pmpro_page_save() function. This makes it possible for unauthenticated attackers to save pages via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2020-36754 MISC MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintech

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/> MISC <https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC <https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-5/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Waiting: One-click countdowns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown name in versions up to, and including, 0.6.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	4.8	CVE-2022-4954 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Theme Switcha plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'theme_switcha_list' shortcode in all versions up to, and including, 3.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5614 MISC <https://plugins.trac.wordpress.org/browser/theme-switcha/tags/3.3/inc/plugin-core.php#l445> MISC MISC <https://plugins.trac.wordpress.org/changeset/2979783/theme-switcha#file1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_delete function. This makes it possible for unauthenticated attackers to delete products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4923 MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l344> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to missing capability checks on the woobe_bulkoperations_delete function. This makes it possible for authenticated attackers, with subscriber access or higher, to delete products.	2023-10-20	4.3	CVE-2023-4924 MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l344> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulk_delete_products function. This makes it possible for unauthenticated attackers to delete products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4926 MISC MISC MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulk/bulk.php#l159>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the create_profile function. This makes it possible for unauthenticated attackers to create profiles via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4935 MISC MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/classes/models/profiles.php#l191> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_apply_default_combination function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4937 MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l286> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_swap function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4940 MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l521> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_swap function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products.	2023-10-20	4.3	CVE-2023-4941 MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l521> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_visibility function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4942 MISC MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l719> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_visibility function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products.	2023-10-20	4.3	CVE-2023-4943 MISC MISC <https://plugins.trac.wordpress.org/browser/woo-bulk-editor/trunk/ext/bulkoperations/bulkoperations.php#l719> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Poptin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'poptin-form' shortcode in versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-4961 MISC MISC <https://plugins.trac.wordpress.org/changeset/2968210/poptin#file2> MISC <https://plugins.trac.wordpress.org/browser/poptin/tags/1.3/poptin.php#l659>
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in POSIMYTH Nexter Extension plugin <= 2.0.3 versions.	2023-10-25	6.1	CVE-2023-45750 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Customizr theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.3.0. This is due to missing or incorrect nonce validation on the czr_fn_post_fields_save() function. This makes it possible for unauthenticated attackers to post fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2020-36755 MISC MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintech

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/> MISC <https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC <https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-5/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Hueman theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.6.3. This is due to missing or incorrect nonce validation on the save_meta_box() function. This makes it possible for unauthenticated attackers to save metabox data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2020-36753 MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://themes.trac.wordpress.org/browser/hueman/3.6.4/option-tree/includes/class-ot-meta-box.php#l207> MISC <https://blog.nintechnet.com/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabil

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ities-part-5/>
wordpress -- wordpress	The Modern Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode in versions up to, and including, 1.4.16 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5618 MISC <https://plugins.trac.wordpress.org/changeset/2980695/modern-footnotes> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Fancy Product Designer plugin for WordPress is vulnerable to unauthorized access to data and modification of plugin settings due to a missing capability check on multiple AJAX functions in versions up to, and including, 4.6.9. This makes it possible for authenticated attackers with subscriber-level permissions to modify plugin settings, including retrieving arbitrary order information or creating/updating/deleting products, orders, or other sensitive information not associated with their own account.	2023-10-20	6.3	CVE-2021-4335 MISC MISC <https://support.fancyproductdesigner.com/support/discussions/topics/13000029981>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Skype Legacy Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'skype-status' shortcode in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5615 MISC MISC <https://plugins.trac.wordpress.org/browser/skype-online-status/tags/3.1/skype-classes.php#l316>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WooCommerce Dynamic Pricing and Discounts plugin for WordPress is vulnerable to unauthenticated settings export in versions up to, and including, 2.4.1. This is due to missing authorization on the export() function which makes makes it possible for unauthenticated attackers to export the plugin's settings.	2023-10-20	5.3	CVE-2021-4353 MISC MISC <https://blog.nintechnet.com/woocommerce-dynamic-pricing-and-discounts-plugin-fixed-multiple-vulnerabilities/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The nsc theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2023-10-20	6.1	CVE-2023-3965 MISC MISC <https://github.com/blackfan/client-side-prototype-pollution>
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Scribit Proofreading plugin <= 1.0.11 versions.	2023-10-25	6.1	CVE-2023-45772 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Podcast Subscribe Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'podcast_subscribe' shortcode in versions up to, and including, 1.4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5308 MISC <https://plugins.trac.wordpress.org/browser/podcast-subscribe-buttons/tags/1.4.8/template-parts/inline-button.php#l30> MISC <https://plugins.trac.wordpress.org/changeset/2973904/podcast-subscribe-buttons#file529> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Website Builder by SeedProd plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.15.13.1. This is due to missing or incorrect nonce validation on functionality in the builder.php file. This makes it possible for unauthenticated attackers to change the stripe connect token via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2023-4975 MISC MISC <https://plugins.trac.wordpress.org/browser/coming-soon/trunk/resources/views/builder.php#l164> MISC <https://plugins.trac.wordpress.org/changeset/2968455/coming-soon/trunk/resources/views/builder.php>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Sitekit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sitekit_iframe' shortcode in versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5071 MISC <https://plugins.trac.wordpress.org/changeset/2970788/sitekit> MISC MISC <https://plugins.trac.wordpress.org/browser/sitekit/trunk/inc/sitekit-shortcode-iframe.php#l3>
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Spider Teams ApplyOnline - Application Form Builder and Manager plugin <= 2.5.2 versions.	2023-10-25	6.1	CVE-2023-45756 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Stephanie Leary Next Page plugin <= 1.5.2 versions.	2023-10-25	4.8	CVE-2023-45768 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Syed Balkhi WP Lightbox 2 plugin <= 3.0.6.5 versions.	2023-10-25	4.8	CVE-2023-45747 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The RSS Aggregator by Feedzy plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4.2. This is due to missing or incorrect nonce validation on the save_feedzy_post_type_meta() function. This makes it possible for unauthenticated attackers to update post meta via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2020-36758 MISC <https://plugins.trac.wordpress.org/changeset/2369394/feedzy-rss-feeds/trunk/includes/admin/feedzy-rss-feeds-admin.php> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://bl

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				og.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				1/> MISC <https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				vulnerabilities-part-5/>
wordpress -- wordpress	The Super Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tpsscode' shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	5.4	CVE-2023-5613 MISC <https://plugins.trac.wordpress.org/browser/super-testimonial/tags/2.8/tp-testimonials.php#l214> MISC <https://plugins.trac.wordpress.org/changeset/2979378/super-testimonial#file9> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.8.5 via the sfsi_save_export function. This can allow subscribers to export plugin settings that include social media authentication tokens and secrets as well as app passwords.	2023-10-20	6.5	CVE-2023-5070 MISC MISC
wordpress -- wordpress	The Modern Events Calendar lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Google API key and Calendar ID in versions up to, but not including, 7.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2023-10-20	4.8	CVE-2023-4021 MISC MISC <https://webnus.net/modern-events-calendar/change-log/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Your Journey theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.9.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2023-10-20	6.1	CVE-2023-3933 MISC <https://github.com/blackfan/client-side-prototype-pollution> MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wokamoto Simple Tweet plugin <= 1.4.0.2 versions.	2023-10-25	4.8	CVE-2023-45767 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Slimstat Analytics plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 5.0.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2023-10-20	6.5	CVE-2023-4598 MISC MISC MISC <https://plugins.trac.wordpress.org/browser/wp-slimstat/tags/5.0.8/admin/view/wp-slimstat-db.php#l970>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WPLegalPages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wplegalpage' shortcode in versions up to, and including, 2.9.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	4.8	CVE-2023-4968 MISC <https://plugins.trac.wordpress.org/changeset/2976774/wplegalpages/trunk/public/class-wp-legal-pages-public.php#file0> MISC MISC <https://plugins.trac.wordpress.org/browser/wplegalpages/tags/2.9.2/public/class-wp-legal-pages-public.php#l150>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Custom CSS, JS & PHP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0.7. This is due to missing or incorrect nonce validation on the save() function. This makes it possible for unauthenticated attackers to save code snippets via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	4.3	CVE-2021-4418 MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/> MISC <https://blog.nintechnet.com/multiple-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				wordpress-plugins-fixed-csrf-vulnerabilities-part-2/> MISC <https://plugins.trac.wordpress.org/browser/custom-css-js-php/trunk/modules/code/model.code.php#l85> MISC MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/> MISC <https://blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabil

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ities-part-5/>
wordpress -- wordpress	The WooCommerce EAN Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the refresh_order_ean_data AJAX action in versions up to 6.1.0. This makes it possible for authenticated attackers with contributor-level access and above, to update EAN numbers for orders.	2023-10-20	4.3	CVE-2023-4947 MISC MISC <https://plugins.yanco.dk/product/woocommerce-ean-payment-gateway/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 0.9.89. This allows authenticated attackers with administrative privileges to delete the contents of arbitrary directories on the server, which can be a critical issue in a shared environments.	2023-10-20	6.5	CVE-2023-4274 MISC <https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/tags/0.9.89/includes/class-wpvivid-setting.php#l200> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the image file path parameter in versions up to, and including, 0.9.89 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-20	4.8	CVE-2023-5120 MISC MISC <https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/tags/0.9.89/includes/upload-cleaner/class-wpvivid-uploads-cleaner.php#l161>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zscaler -- client_connector	An authentication bypass by spoofing of a device with a synthetic IP address is possible in Zscaler Client Connector on Windows, allowing a functionality bypass. This issue affects Client Connector: before 3.9.	2023-10-23	6.5	CVE-2023-28803 MISC <https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023>
zscaler -- client_connector	Zscaler Client Connector Installer on Windows before version 3.4.0.124 improperly handled directory junctions during uninstallation. A local adversary may be able to delete folders in an elevated context.	2023-10-23	5.5	CVE-2021-26734 MISC <https://help.zscaler.com/zscaler-client-connector/client-connector-app-release-summary-2021>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zscaler -- client_connector	An Improper Verification of Cryptographic Signature vulnerability in Zscaler Client Connector on Linux allows replacing binaries.This issue affects Linux Client Connector: before 1.4.0.105	2023-10-23	5.3	CVE-2023-28804 MISC <https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023>
zscaler -- client_connector	The Zscaler Client Connector for macOS prior to 3.6 did not sufficiently validate RPC clients. A local adversary without sufficient privileges may be able to shutdown the Zscaler tunnel by exploiting a race condition.	2023-10-23	4.7	CVE-2021-26737 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
There were no low vulnerabilities recorded this week.				

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abus_group -- tvip	An issue was discovered on certain ABUS TVIP devices. Due to a path traversal in /opt/cgi/admin/filewrite, an attacker can write to files, and thus execute code arbitrarily with root privileges.	2023-10-26	not yet calculated	CVE-2018-16739 MISC <https://sec.maride.cc/posts/abus/> MISC <https://www.ccc.de/en/updates/2019/update-nicht-verfugbar-hersteller-nicht-zu-erreichen>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abus_group -- tvip	Hardcoded manufacturer credentials and an OS command injection vulnerability in the /cgi-bin/mft/ directory on ABUS TVIP TVIP20050 LM.1.6.18, TVIP10051 LM.1.6.18, TVIP11050 MG.1.6.03.05, TVIP20550 LM.1.6.18, TVIP10050 LM.1.6.18, TVIP11550 MG.1.6.03, TVIP21050 MG.1.6.03, and TVIP51550 MG.1.6.03 cameras allow remote attackers to execute code as root.	2023-10-26	not yet calculated	CVE-2018-17558 MISC <https://sec.maride.cc/posts/abus/> MISC <https://www.ccc.de/en/updates/2019/update-nicht-verfugbar-hersteller-nicht-zu-erreichen>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abus_group -- tvip	Due to incorrect access control, unauthenticated remote attackers can view the /video.mjpg video stream of certain ABUS TVIP cameras.	2023-10-26	not yet calculated	CVE-2018-17559 MISC <https://sec.maride.cc/posts/abus/#cve-2018-17559> MISC <https://www.ccc.de/en/updates/2019/update-nicht-verfugbar-hersteller-nicht-zu-erreichen>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abus_group -- tvip	Buffer Overflow vulnerability in certain ABUS TVIP cameras allows attackers to gain control of the program via crafted string sent to sprintf() function.	2023-10-26	not yet calculated	CVE-2018-17878 MISC <https://sec.maride.cc/posts/abus/#cve-2018-17878> MISC <https://www.ccc.de/en/updates/2019/update-nicht-verfugbar-hersteller-nicht-zu-erreichen>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abus_group -- tvip	An issue was discovered on certain ABUS TVIP cameras. The CGI scripts allow remote attackers to execute code via system() as root. There are several injection points in various scripts.	2023-10-26	not yet calculated	CVE-2018-17879 MISC <https://sec.maride.cc/posts/abus/#cve-2018-17879> MISC <https://www.ccc.de/en/updates/2019/update-nicht-verfugbar-hersteller-nicht-zu-erreichen>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
agevolt_slovakia_s.r.o. -- agevolt_portal	An arbitrary file upload and directory traversal vulnerability exist in the file upload functionality of the System Setup menu in AgeVolt Portal prior to version 0.1. A remote authenticated attacker could leverage this vulnerability to upload files to any location on the target operating system with web server privileges.	2023-10-25	not yet calculated	CVE-2022-38484 MISC <https://citadelo.com/download/cve-2022-38484.pdf>
agevolt_slovakia_s.r.o. -- agevolt_portal	A directory traversal vulnerability exists in the AgeVolt Portal prior to version 0.1 that leads to Information Disclosure. A remote authenticated attacker could leverage this vulnerability to read files from any location on the target operating system with web server privileges.	2023-10-25	not yet calculated	CVE-2022-38485 MISC <https://citadelo.com/download/cve-2022-38485.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2023-10-25	not yet calculated	CVE-2023-42488 MISC <https://www.gov.il/en/departments/faq/cve_advisories>
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-732: Incorrect Permission Assignment for Critical Resource	2023-10-25	not yet calculated	CVE-2023-42489 MISC <https://www.gov.il/en/departments/faq/cve_advisories>
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2023-10-25	not yet calculated	CVE-2023-42490 MISC <https://www.gov.il/en/departments/faq/cve_advisories>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-285: Improper Authorization	2023-10-25	not yet calculated	CVE-2023-42491 MISC <https://www.gov.il/en/departments/faq/cve_advisories>
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-321: Use of Hard-coded Cryptographic Key	2023-10-25	not yet calculated	CVE-2023-42492 MISC <https://www.gov.il/en/departments/faq/cve_advisories>
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-256: Plaintext Storage of a Password	2023-10-25	not yet calculated	CVE-2023-42493 MISC <https://www.gov.il/en/departments/faq/cve_advisories>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alexander_maier_gmbh -- eisbaer_scada	EisBaer Scada - CWE-749: Exposed Dangerous Method or Function	2023-10-25	not yet calculated	CVE-2023-42494 MISC <https://www.gov.il/en/departments/faq/cve_advisories>
anglaise.company -- anglaise.company	An issue in Anglaise Company Anglaise.Company v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	2023-10-25	not yet calculated	CVE-2023-38845 MISC <https://liff.line.me/1657030660-8ndeqnbe> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-38845.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- activemq	Apache ActiveMQ is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Users are recommended to upgrade to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.	2023-10-27	not yet calculated	CVE-2023-46604 MISC <https://activemq.apache.org/security-advisories.data/cve-2023-46604-announcement.txt> MISC <http://www.openwall.com/lists/oss-security/2023/10/27/5>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- airflow_celery	Insertion of Sensitive Information into Log File vulnerability in Apache Airflow Celery provider, Apache Airflow. Sensitive information logged as clear text when rediss, amqp, rpc protocols are used as Celery result backend Note: the vulnerability is about the information exposed in the logs not about accessing the logs. This issue affects Apache Airflow Celery provider: from 3.3.0 through 3.4.0; Apache Airflow: from 1.10.0 through 2.6.3. Users are recommended to upgrade Airflow Celery provider to version 3.4.1 and Apache Airlfow to version 2.7.0 which fixes the issue.	2023-10-28	not yet calculated	CVE-2023-46215 MISC <https://github.com/apache/airflow/pull/34954> MISC <https://lists.apache.org/thread/wm1jfmks7r6m7bj0mq4lmw3998svn46n> MISC <http://www.openwall.com/lists/oss-security/2023/10/28/1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- http_server	An attacker, opening a HTTP/2 connection with an initial window size of 0 was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well-known "slow loris" attack pattern. This has been fixed in version 2.4.58 so that such connections are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.	2023-10-23	not yet calculated	CVE-2023-43622 MISC <https://httpd.apache.org/security/vulnerabilities_24.html> MISC <https://security.netapp.com/advisory/ntap-20231027-0011/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- http_server	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.	2023-10-23	not yet calculated	CVE-2023-45802 MISC <https://httpd.apache.org/security/vulnerabilities_24.html> MISC <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/bfqd3kuemfbhpapbglwqc34l4owl5haz/> MISC <https://security.netapp.com/advisory/ntap-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				20231027-0011/>
apple -- ios/ipados	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2. A user's password may be read aloud by VoiceOver.	2023-10-25	not yet calculated	CVE-2023-32359 MISC <https://support.apple.com/en-us/ht213981> MISC <http://seclists.org/fulldisclosure/2023/oct/23>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ios/ipados	The issue was addressed with improved UI handling. This issue is fixed in iOS 17.1 and iPadOS 17.1. A device may persistently fail to lock.	2023-10-25	not yet calculated	CVE-2023-40445 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/kb/ht213982> MISC <http://seclists.org/fulldisclosure/2023/oct/19>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.6.1. An attacker may be able to access passkeys without authentication.	2023-10-25	not yet calculated	CVE-2023-40401 MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/26>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges.	2023-10-25	not yet calculated	CVE-2023-40404 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1. An app may be able to read sensitive location information.	2023-10-25	not yet calculated	CVE-2023-40405 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-40421 MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/21> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Monterey 12.7.1. An app with root privileges may be able to access private information.	2023-10-25	not yet calculated	CVE-2023-40425 MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/kb/ht213983> MISC <http://seclists.org/fulldisclosure/2023/oct/21>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1. An app may be able to access user-sensitive data.	2023-10-25	not yet calculated	CVE-2023-40444 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6.1. An app may be able to access protected user data.	2023-10-25	not yet calculated	CVE-2023-41077 MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/26>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access the microphone without the microphone use indicator being shown.	2023-10-25	not yet calculated	CVE-2023-41975 MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/21> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14.1, iOS 16.7.2 and iPadOS 16.7.2. Visiting a malicious website may reveal browsing history.	2023-10-25	not yet calculated	CVE-2023-41977 MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/24>
apple -- macos	The issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1. An attacker may be able to execute arbitrary code as root from the Lock Screen.	2023-10-25	not yet calculated	CVE-2023-41989 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. Visiting a malicious website may lead to user interface spoofing.	2023-10-25	not yet calculated	CVE-2023-42438 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-42842 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-42850 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. An attacker with knowledge of a standard user's credentials can unlock another standard user's locked screen on the same Mac.	2023-10-25	not yet calculated	CVE-2023-42861 MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly.	2023-10-25	not yet calculated	CVE-2023-40408 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information.	2023-10-25	not yet calculated	CVE-2023-40413 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclosure/2023/oct/21>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory.	2023-10-25	not yet calculated	CVE-2023-40416 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213983> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.ap

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/21>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges.	2023-10-25	not yet calculated	CVE-2023-40423 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213983> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.ap

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/21>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	2023-10-25	not yet calculated	CVE-2023-40447 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213986> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213987> MISC <https://support.apple.com/en-us/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/27> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://se

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				clists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclosure/2023/oct/22>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service.	2023-10-25	not yet calculated	CVE-2023-40449 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213983> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.ap

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/21>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-41072 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-41254 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <https://support.ap

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	2023-10-25	not yet calculated	CVE-2023-41976 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213986> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213987> MISC <https://support.apple.com/en-us/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/27> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://se

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				clists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclosure/2023/oct/22>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-41982 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service.	2023-10-25	not yet calculated	CVE-2023-41983 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213986> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/27> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-41988 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213982> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-41997 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213984> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges.	2023-10-25	not yet calculated	CVE-2023-42841 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access sensitive user data when resolving symlinks.	2023-10-25	not yet calculated	CVE-2023-42844 MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/21> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. Photos in the Hidden Photos Album may be viewed without authentication.	2023-10-25	not yet calculated	CVE-2023-42845 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address.	2023-10-25	not yet calculated	CVE-2023-42846 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213987> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213987> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclos

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ure/2023/oct/22> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/oct/19>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An attacker may be able to access passkeys without authentication.	2023-10-25	not yet calculated	CVE-2023-42847 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	2023-10-25	not yet calculated	CVE-2023-42849 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213981> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <https://support.apple.com/kb/ht213988> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://seclists.org/fulldisclosure/2023/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclosure/2023/oct/21>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	2023-10-25	not yet calculated	CVE-2023-42852 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213981> MISC <https://support.apple.com/en-us/ht213988> MISC <https://support.apple.com/en-us/ht213986> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<https://support.apple.com/en-us/ht213987> MISC <https://support.apple.com/en-us/ht213984> MISC <http://seclists.org/fulldisclosure/2023/oct/23> MISC <http://seclists.org/fulldisclosure/2023/oct/27> MISC <http://seclists.org/fulldisclosure/2023/oct/25> MISC <http://se

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				clists.org/fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24> MISC <http://seclists.org/fulldisclosure/2023/oct/22>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to cause a denial-of-service to Endpoint Security clients.	2023-10-25	not yet calculated	CVE-2023-42854 MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/21> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. Processing a file may lead to unexpected app termination or arbitrary code execution.	2023-10-25	not yet calculated	CVE-2023-42856 MISC <https://support.apple.com/en-us/ht213983> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/en-us/ht213985> MISC <https://support.apple.com/kb/ht213983> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				upport.apple.com/kb/ht213984> MISC <https://support.apple.com/kb/ht213985> MISC <http://seclists.org/fulldisclosure/2023/oct/21> MISC <http://seclists.org/fulldisclosure/2023/oct/26> MISC <http://seclists.org/fulldisclosure/2023/oct/24>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	2023-10-25	not yet calculated	CVE-2023-42857 MISC <https://support.apple.com/en-us/ht213982> MISC <https://support.apple.com/en-us/ht213984> MISC <https://support.apple.com/kb/ht213982> MISC <https://support.apple.com/kb/ht213984> MISC <http://seclists.org/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				fulldisclosure/2023/oct/19> MISC <http://seclists.org/fulldisclosure/2023/oct/24>
ashlar-vellum -- graphite	In Ashlar-Vellum Graphite v13.0.48, the affected application lacks proper validation of user-supplied data when parsing VC6 files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	2023-10-26	not yet calculated	CVE-2023-39936 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-03>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ashlar-vellum -- multiple_products	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share v12 SP0 Build (1204.77), the affected applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	2023-10-26	not yet calculated	CVE-2023-39427 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-03>
audimex -- audimex	Audimex 15.0.0 is vulnerable to Cross Site Scripting (XSS) in /audimex/cgi-bin/wal.fcgi via company parameter search filters.	2023-10-25	not yet calculated	CVE-2023-46396 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
basercms -- basercms	baserCMS is a website development framework with WebAPI that runs on PHP8 and CakePHP4. There is a XSS Vulnerability in Favorites Feature to baserCMS. This issue has been patched in version 4.8.0.	2023-10-27	not yet calculated	CVE-2023-29009 MISC <https://github.com/baserproject/basercms/releases/tag/basercms-4.8.0> MISC <https://basercms.net/security/jvn_45547161> MISC <https://github.com/baserproject/basercms/security/advisories/ghsa-8vqx-prq4-rqrq>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bosch_rexroth_ag -- ctrlx_hmi_web_pane	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device	2023-10-25	not yet calculated	CVE-2023-45851 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bosch_rexroth_ag -- ctrlx_hmi_web_panel	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol.	2023-10-25	not yet calculated	CVE-2023-45321 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bosch_rexroth_ag -- ctrlx_hmi_web_panel	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself.	2023-10-25	not yet calculated	CVE-2023-46102 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
browserify -- browserify	browserify-sign is a package to duplicate the functionality of node's crypto public key functions, much of this is based on Fedor Indutny's work on indutny/tls.js. An upper bound check issue in `dsaVerify` function allows an attacker to construct signatures that can be successfully verified by any public key, thus leading to a signature forgery attack. All places in this project that involve DSA verification of user-input signatures will be affected by this vulnerability. This issue has been patched in version 4.2.2.	2023-10-26	not yet calculated	CVE-2023-46234 MISC <https://github.com/browserify/browserify-sign/security/advisories/ghsa-x9w5-v3q2-3rhw> MISC <https://github.com/browserify/browserify-sign/commit/85994cd6348b50f2fd1b73c54e20881416f44a30> MISC <https://lists.debian.org/debia

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				n-lts-announce/2023/10/msg00040.html>
cacti -- cacti	SQL Injection vulnerability in Cacti v1.2.25 allows a remote attacker to obtain sensitive information via the form_actions() function in the managers.php function.	2023-10-27	not yet calculated	CVE-2023-46490 MISC <https://gist.github.com/ishgard-2/a95632111138fcd7ccf7432ccb145b53> MISC <https://github.com/cacti/cacti/security/advisories/ghsa-f4r3-53jr-654c>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
carrental -- carrental	carRental 1.0 is vulnerable to Incorrect Access Control (Arbitrary File Read on the Back-end System).	2023-10-23	not yet calculated	CVE-2023-33517 MISC <https://gist.github.com/wushigudan/288ab32566615d8897c1da7ce7204838>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cassia_networks -- access_controller	An issue was discovered in Cassia Access Controller 2.1.1.2303271039. The Web SSH terminal endpoint (spawned console) can be accessed without authentication. Specifically, there is no session cookie validation on the Access Controller; instead, there is only Basic Authentication to the SSH console.	2023-10-27	not yet calculated	CVE-2023-35794 MISC <https://github.com/dodge-mptc/cve-2023-35794-webssh-hijacking> MISC <https://www.cassianetworks.com/products/iot-access-controller/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
catdoc -- catdoc	Catdoc v0.95 was discovered to contain a NULL pointer dereference via the component xls2csv at src/xlsparse.c.	2023-10-26	not yet calculated	CVE-2023-46345 MISC <https://gist.github.com/rycbar77/d747b2c37b544ece30b2353a65ab41f9>
christina_japan_line -- christina_japan_line	An issue in CHRISTINA JAPAN Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	2023-10-25	not yet calculated	CVE-2023-38847 MISC <https://liff.line.me/1657631315-ox5j26ak> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-38847.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- cisco_ios_xe_software	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	2023-10-25	not yet calculated	CVE-2023-20273 MISC <https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-iosxe-webui-privesc-j22saa4z>
cloud_software_group -- netscaler_adc/gateway	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server	2023-10-27	not yet calculated	CVE-2023-4967 MISC <https://support.citrix.com/article/ctx579459/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	An issue in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted payload to the Content Manager Menu component.	2023-10-26	not yet calculated	CVE-2023-43352 MISC <https://github.com/sromanhu/cve-2023-43352-cmsmadesimple-ssti--content> MISC <https://github.com/sromanhu/cmsmadesimple-ssti--content>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Title parameter in the News Menu component.	2023-10-23	not yet calculated	CVE-2023-43358 MISC <https://github.com/sromanhu/cve-2023-43358-cmsmadesimple-stored-xss---news> MISC <https://github.com/sromanhu/cmsmadesimple-stored-xss---news>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cmsmadesimple	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Top Directory parameter in the File Picker Menu component.	2023-10-25	not yet calculated	CVE-2023-43360 MISC <https://github.com/sromanhu/cmsmadesimple-stored-xss---file-picker-extension> MISC <https://github.com/sromanhu/cve-2023-43360-cmsmadesimple-stored-xss---file-picker-extension>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- admission_management_system	A vulnerability was found in code-projects Admission Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file student_avatar.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243728.	2023-10-27	not yet calculated	CVE-2023-5829 MISC MISC MISC <https://github.com/lxxcute/bug/blob/main/admission%20management%20system%20has%20a%20file%20upload%20(rce)%20vulnerability.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codeastro -- pos_system	A vulnerability was found in CodeAstro POS System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /profil of the component Profile Picture Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243601 was assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5795 MISC MISC MISC
codeastro -- pos_system	A vulnerability was found in CodeAstro POS System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /setting of the component Logo Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-243602 is the identifier assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5796 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
coderedcorp -- wagtail_crx	views.py in Wagtail CRX CodeRed Extensions (formerly CodeRed CMS or coderedcms) before 0.22.3 allows upward protected/..%2f..%2f path traversal when serving protected media.	2023-10-22	not yet calculated	CVE-2021-46897 MISC <https://github.com/coderedcorp/coderedcms/issues/448> MISC <https://github.com/coderedcorp/coderedcms/pull/450> MISC <https://github.com/coderedcorp/coderedcms/compare/v0.22.2...v0.22.3>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
columbiasoft -- document_locator	A vulnerability classified as critical has been found in ColumbiaSoft Document Locator. This affects an unknown part of the file /api/authentication/login of the component WebTools. The manipulation of the argument Server leads to improper authentication. It is possible to initiate the attack remotely. Upgrading to version 7.2 SP4 and 2021.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243729 was assigned to this vulnerability.	2023-10-27	not yet calculated	CVE-2023-5830 MISC MISC
concrete_cms -- concrete_cms	Multiple Cross Site Scripting (XSS) vulnerabilities in Concrete CMS v.9.2.1 allow an attacker to execute arbitrary code via a crafted script to the Header and Footer Tracking Codes of the SEO & Statistics.	2023-10-23	not yet calculated	CVE-2023-44760 MISC <https://github.com/sromanhu/concretecms-stored-xss---trackingcodes>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contec_co._ltd. -- solarview_compact	An issue in Contec SolarView Compact v.6.0 and before allows an attacker to execute arbitrary code via the texteditor.php component.	2023-10-27	not yet calculated	CVE-2023-46509 MISC <https://gist.github.com/atonysan/d6f72e9eb90407d64bed4566aa80afb1#file-cve-2023-46509>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
crypto-es -- crypto-es	CryptoES is a cryptography algorithms library compatible with ES6 and TypeScript. Prior to version 2.1.0, CryptoES PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 2.1.0 contains a patch for this issue. As a workaround, configure CryptoES to use SHA256 with at least 250,000 iterations.	2023-10-25	not yet calculated	CVE-2023-46133 MISC <https://github.com/entronad/crypto-es/commit/d506677fae3d03a454b37ad126e0c119d416b757> MISC <https://github.com/entronad/crypto-es/security/advisories/ghsa-mpj8-q39x-wq5h>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
crypto-js -- crypto-js	crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains a patch for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations.	2023-10-25	not yet calculated	CVE-2023-46233 MISC <https://github.com/brix/crypto-js/security/advisories/ghsa-xwcq-pm8m-c4vf> MISC <https://github.com/brix/crypto-js/commit/421dd538b2d34e7c24a5b72cc64dc2b9167db40a>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dar-7000	SQL injection vulnerability in D-Link Online behavior audit gateway DAR-7000 V31R02B1413C allows a remote attacker to obtain sensitive information and execute arbitrary code via the editrole.php component.	2023-10-26	not yet calculated	CVE-2023-42406 MISC <https://github.com/flyyue2001/cve/blob/main/d-link%20-dar-7000_sql_:sysmanage:editrole.php.md> MISC <https://github.com/1dreamgn/cve/blob/main/cve-2023-42406.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
deciso_b.v. -- opnsense	DECISO OPNsense 23.1 does not impose rate limits for authentication, allowing attackers to perform a brute-force attack to bypass authentication.	2023-10-23	not yet calculated	CVE-2023-27152 MISC <https://www.esecforte.com/cve-2023-27152-opnsense-brute-force/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
django_grappelli -- django_grappelli	views/switch.py in django-grappelli (aka Django Grappelli) before 2.15.2 attempts to prevent external redirection with startswith("/") but this does not consider a protocol-relative URL (e.g., //example.com) attack.	2023-10-22	not yet calculated	CVE-2021-46898 MISC <https://github.com/sehmaschine/django-grappelli/commit/4ca94bcda0fa272059450685 3d85e00c8212968f> MISC <https://github.com/sehmaschine/django-grappelli/pull/976> MISC <https://github.com/sehmaschine/django-grappelli/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				compare/2.15.1...2.15.2> MISC <https://github.com/sehmaschine/django-grappelli/issues/975>
dragon_path -- 707gr1	A vulnerability classified as problematic has been found in Dragon Path 707GR1 up to 20231022. Affected is an unknown function of the component Ping Diagnostics. The manipulation of the argument Host Address with the input >><img/src/onerror=alert(1)> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-243594 is the identifier assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5789 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dromara_sureness -- dromara_sureness	Dromara Sureness before v1.0.8 was discovered to use a hardcoded key.	2023-10-25	not yet calculated	CVE-2023-31581 MISC <https://github.com/dromara/sureness/issues/164> MISC <https://github.com/xubowenw/jwtissues/blob/main/sureness%20secure%20issues.md>
egroupware -- egroupware	An issue was discovered in eGroupWare 17.1.20190111. An Improper Password Storage vulnerability affects the setup panel of under setup/manageheader.php, which allows authenticated remote attackers with administrator credentials to read a cleartext database password.	2023-10-26	not yet calculated	CVE-2023-38328 MISC <https://www.gruppotim.it/it/footer/red-team.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- beats	It was discovered that when acting as TLS clients, Beats, Elastic Agent, APM Server, and Fleet Server did not verify whether the server certificate is valid for the target IP address; however, certificate signature validation is still performed. More specifically, when the client is configured to connect to an IP address (instead of a hostname) it does not validate the server certificate's IP SAN values against that IP address and certificate validation fails, and therefore the connection is not blocked as expected.	2023-10-26	not yet calculated	CVE-2023-31421 MISC <https://discuss.elastic.co/t/beats-elastic-agent-apm-server-and-fleet-server-8-10-1-security-update-improper-certificate-validation-issue-esa-2023-16/343385> MISC <https://www.elastic.co/community/security>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- elastic_cloud_on_kubernetes	Secret token configuration is never applied when using ECK <2.8 with APM Server >=8.0. This could lead to anonymous requests to an APM Server being accepted and the data ingested into this APM deployment.	2023-10-26	not yet calculated	CVE-2023-31416 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/elastic-cloud-on-kubernetes-eck-2-8-security-update/343854>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- elastic_sharepoint_online_python_connector	An issue was discovered when using Document Level Security and the SPO "Limited Access" functionality in Elastic Sharepoint Online Python Connector. If a user is assigned limited access permissions to an item on a SharePoint site then that user would have read permissions to all content on the Sharepoint site through Elasticsearch.	2023-10-26	not yet calculated	CVE-2023-46666 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/elastic-sharepoint-online-python-connector-v8-10-3-0-security-update/344732>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- elasticsearch	Elasticsearch generally filters out sensitive information and credentials before logging to the audit log. It was found that this filtering was not applied when requests to Elasticsearch use certain deprecated URIs for APIs. The impact of this flaw is that sensitive information such as passwords and tokens might be printed in cleartext in Elasticsearch audit logs. Note that audit logging is disabled by default and needs to be explicitly enabled and even when audit logging is enabled, request bodies that could contain sensitive information are not printed to the audit log unless explicitly configured.	2023-10-26	not yet calculated	CVE-2023-31417 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/elasticsearch-8-9-2-and-7-17-13-security-update/342479>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- elasticsearch	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user could force an Elasticsearch node to exit with an OutOfMemory error by sending a moderate number of malformed HTTP requests. The issue was identified by Elastic Engineering and we have no indication that the issue is known or that it is being exploited in the wild.	2023-10-26	not yet calculated	CVE-2023-31418 MISC <https://discuss.elastic.co/t/elasticsearch-8-9-0-7-17-13-security-update/343616> MISC <https://www.elastic.co/community/security>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- elasticsearch	A flaw was discovered in Elasticsearch, affecting the _search API that allowed a specially crafted query string to cause a Stack Overflow and ultimately a Denial of Service.	2023-10-26	not yet calculated	CVE-2023-31419 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/elasticsearch-8-9-1-7-17-13-security-update/343297>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- endpoint	If Elastic Endpoint (v7.9.0 - v8.10.3) is configured to use a non-default option in which the logging level is explicitly set to debug, and when Elastic Agent is simultaneously configured to collect and send those logs to Elasticsearch, then Elastic Agent API keys can be viewed in Elasticsearch in plaintext. These API keys could be used to write arbitrary data and read Elastic Endpoint user artifacts.	2023-10-26	not yet calculated	CVE-2023-46668 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/endpoint-v8-10-4-security-update/345203>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- fleet_server	An issue was discovered in Fleet Server >= v8.10.0 and < v8.10.3 where Agent enrolment tokens are being inserted into the Fleet Server's log file in plain text. These enrolment tokens could allow someone to enroll an agent into an agent policy, and potentially use that to retrieve other secrets in the policy including for Elasticsearch and third-party services. Alternatively a threat actor could potentially enrol agents to the clusters and send arbitrary events to Elasticsearch.	2023-10-26	not yet calculated	CVE-2023-46667 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/fleet-server-v8-10-3-security-update/344737>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elastic -- kibana	An issue was discovered by Elastic whereby sensitive information is recorded in Kibana logs in the event of an error. The issue impacts only Kibana version 8.10.0 when logging in the JSON layout or when the pattern layout is configured to log the %meta pattern. Elastic has released Kibana 8.10.1 which resolves this issue. The error object recorded in the log contains request information, which can include sensitive data, such as authentication credentials, cookies, authorization headers, query params, request paths, and other metadata. Some examples of sensitive data which can be included in the logs are account credentials for kibana_system, kibana-metricbeat, or Kibana end-users.	2023-10-26	not yet calculated	CVE-2023-31422 MISC <https://www.elastic.co/community/security> MISC <https://discuss.elastic.co/t/kibana-8-10-1-security-update/343287>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
exfatprogs -- exfatprogs	exfatprogs before 1.2.2 allows out-of-bounds memory access, such as in read_file_dentry_set.	2023-10-28	not yet calculated	CVE-2023-45897 MISC <https://github.com/exfatprogs/exfatprogs/commit/22d0e43e8d24119cbfc6efafabb0dec6517a86c4> MISC <https://github.com/exfatprogs/exfatprogs/releases/tag/1.2.2> MISC <https://github.com/exfatprogs/exfatprogs/commit/4abc55e976573991e6a1117

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				bb2b3711e59da07ae> MISC <https://github.com/exfatprogs/exfatprogs/commit/ec78688e5fb5a70e13df82b4c0da1e6228d3ccdf>
fancms -- fancms	Cross Site Scripting vulnerability in FanCMS v.1.0.0 allows an attacker to execute arbitrary code via the content1 parameter in the demo.php file.	2023-10-27	not yet calculated	CVE-2023-46505 MISC <https://github.com/pwncyn/fancms/issues/1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ffmpeg -- ffmpeg	FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	2023-10-27	not yet calculated	CVE-2023-46407 MISC <https://github.com/ffmpeg/ffmpeg/commit/bf814387f42e9b0dea9d75c03db4723c88e7d962> MISC <https://patchwork.ffmpeg.org/project/ffmpeg/patch/20231013014959.536776-1-leo.izen@gmail.com/> MISC <https://patchwork.ffmpeg.org/project/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ffmpeg/patch/20231015004924.597746-1-leo.izen@gmail.com/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fides -- fides	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in runtime environments, and the enforcement of privacy regulations in code. The Fides web application allows a custom integration to be uploaded as a ZIP file containing configuration and dataset definitions in YAML format. It was discovered that specially crafted YAML dataset and config files allow a malicious user to perform arbitrary requests to internal systems and exfiltrate data outside the environment (also known as a Server-Side Request Forgery). The application does not perform proper validation to block attempts to connect to internal (including localhost) resources. The vulnerability has been patched in Fides version `2.22.1`.	2023-10-25	not yet calculated	CVE-2023-46124 MISC <https://github.com/ethyca/fides/releases/tag/2.22.1> MISC <https://github.com/ethyca/fides/commit/cd344d016b1441662a61d0759e7913e8228ed1ee> MISC <https://github.com/ethyca/fides/security/advisories/ghsa-jq3w-9mgf-43m4>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fides -- fides	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in a runtime environment, and the enforcement of privacy regulations in code. The Fides webserver API allows users to retrieve its configuration using the `GET api/v1/config` endpoint. The configuration data is filtered to suppress most sensitive configuration information before it is returned to the user, but even the filtered data contains information about the internals and the backend infrastructure, such as various settings, servers' addresses and ports and database username. This information is useful for administrative users as well as attackers, thus it should not be revealed to low-privileged users. This vulnerability allows Admin UI users with roles lower than the owner role e.g. the viewer role to retrieve the config information using the API. The vulnerability has been patched in Fides version `2.22.1`.	2023-10-25	not yet calculated	CVE-2023-46125 MISC <https://github.com/ethyca/fides/commit/c9f3a620a4b4c1916e0941cb5624dcd636f06d06> MISC <https://github.com/ethyca/fides/security/advisories/ghsa-rjxg-rpg3-9r89> MISC <https://github.com/ethyca/fides/releases/tag/2.22.1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fides -- fides	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in runtime environments, helping enforce privacy regulations in code. The Fides web application allows users to edit consent and privacy notices such as cookie banners. The vulnerability makes it possible to craft a payload in the privacy policy URL which triggers JavaScript execution when the privacy notice is served by an integrated website. The domain scope of the executed JavaScript is that of the integrated website. Exploitation is limited to Admin UI users with the contributor role or higher. The vulnerability has been patched in Fides version `2.22.1`.	2023-10-25	not yet calculated	CVE-2023-46126 MISC <https://github.com/ethyca/fides/security/advisories/ghsa-fgjj-5jmr-gh83> MISC <https://github.com/ethyca/fides/releases/tag/2.22.1> MISC <https://github.com/ethyca/fides/commit/3231d19699f9c895c986f6a967a64d882769c506>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flusity_cms -- flusity_cms	A vulnerability was found in flusity CMS and classified as problematic. This issue affects the function loadCustomBlocCreateForm of the file /core/tools/customblock.php of the component Dashboard. The manipulation of the argument customblock_place leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 81252bc764e1de2422e79e36194bba1289e7a0a5. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-243599.	2023-10-26	not yet calculated	CVE-2023-5793 MISC <https://github.com/flusity/flusity-cms/commit/81252bc764e1de2422e79e36194bba1289e7a0a5> MISC MISC <https://github.com/flusity/flusity-cms/issues/1> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flusity_cms -- flusity_cms	A vulnerability, which was classified as problematic, has been found in flusity CMS. This issue affects the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument edit_post_id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 6943991c62ed87c7a57989a0cb7077316127def8. It is recommended to apply a patch to fix this issue. The identifier VDB-243641 was assigned to this vulnerability.	2023-10-27	not yet calculated	CVE-2023-5810 MISC <https://github.com/flusity/flusity-cms/issues/2> MISC <https://github.com/flusity/flusity-cms/commit/6943991c62ed87c7a57989a0cb7077316127def8> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flusity_cms -- flusity_cms	A vulnerability, which was classified as problematic, was found in flusity CMS. Affected is the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument menu_id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as 6943991c62ed87c7a57989a0cb7077316127def8. It is recommended to apply a patch to fix this issue. VDB-243642 is the identifier assigned to this vulnerability.	2023-10-27	not yet calculated	CVE-2023-5811 MISC <https://github.com/flusity/flusity-cms/commit/6943991c62ed87c7a57989a0cb7077316127def8> MISC <https://github.com/flusity/flusity-cms/issues/3> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flusity_cms -- flusity_cms	A vulnerability has been found in flusity CMS and classified as critical. Affected by this vulnerability is the function handleFileUpload of the file core/tools/upload.php. The manipulation of the argument uploaded_file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-243643.	2023-10-27	not yet calculated	CVE-2023-5812 MISC MISC MISC <https://github.com/flusity/flusity-cms/issues/4>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fotoscms2 -- fotoscms2	A vulnerability classified as problematic was found in AlexanderLivanov FotosCMS2 up to 2.4.3. This vulnerability affects unknown code of the file profile.php of the component Cookie Handler. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243802 is the identifier assigned to this vulnerability.	2023-10-28	not yet calculated	CVE-2023-5837 MISC MISC MISC <https://github.com/alexanderlivanov/fotoscms2/issues/18>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frappe -- frappe	Frappe is a full-stack web application framework that uses Python and MariaDB on the server side and an integrated client side library. A malicious Frappe user with desk access could create documents containing HTML payloads allowing HTML Injection. This vulnerability has been patched in version 14.49.0.	2023-10-23	not yet calculated	CVE-2023-46127 MISC <https://github.com/frappe/frappe/pull/22339> MISC <https://github.com/frappe/frappe/commit/3dc5d2fcc7561dde181ba953009fe6e39d64e900> MISC <https://github.com/frappe/frappe/security/advisories/ghsa-j2w9-8xrr-7g98>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
free5gc -- free5gc	pkg/suci/suci.go in free5GC udm before 1.2.0, when Go before 1.19 is used, allows an Invalid Curve Attack because it may compute a shared secret via an uncompressed public key that has not been validated. An attacker can send arbitrary SUCIs to the UDM, which tries to decrypt them via both its private key and the attacker's public key.	2023-10-23	not yet calculated	CVE-2023-46324 MISC <https://github.com/free5gc/udm/pull/20> MISC <https://github.com/free5gc/udm/compare/v1.1.1...v1.2.0>
frrouting_frr -- frrouting_frr	An issue was discovered in FRRouting FRR through 9.0.1. It mishandles malformed MP_REACH_NLRI data, leading to a crash.	2023-10-26	not yet calculated	CVE-2023-46752 MISC <https://github.com/frrouting/frr/pull/14645/commits/b08afc81c60607a4f736f418f2e3eb06087f1a35>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frrouting_frr -- frrouting_frr	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur for a crafted BGP UPDATE message without mandatory attributes, e.g., one with only an unknown transit attribute.	2023-10-26	not yet calculated	CVE-2023-46753 MISC <https://github.com/frrouting/frr/pull/14645/commits/d8482bf011cb2b173e85b65b4bf3d5061250cdb9>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fukunaga_memberscard_line -- fukunaga_memberscard_line	The leakage of the client secret in Fukunaga_memberscard Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39736 MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39736.md> MISC <https://liff.line.me/1657606123-4kp0xvrp>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
geeklog -- geeklog	Cross Site Scripting (XSS) vulnerability in Geeklog-Core geeklog v.2.2.2 allows a remote attacker to execute arbitrary code via a crafted payload to the grp_desc parameter of the admin/group.php component.	2023-10-24	not yet calculated	CVE-2023-46058 MISC <https://github.com/crownztx/vulnerabilities/blob/main/geeklog/stored_xss_in_group.php.md>
geeklog -- geeklog	Cross Site Scripting (XSS) vulnerability in Geeklog-Core geeklog v.2.2.2 allows a remote attacker to execute arbitrary code via a crafted payload to the Service, and website URL to Ping parameters of the admin/trackback.php component.	2023-10-24	not yet calculated	CVE-2023-46059 MISC <https://github.com/crownztx/vulnerabilities/blob/main/geeklog/reflected_xss_in_editservice.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The WMS specification defines an ``sld=<url>`` parameter for GetMap, GetLegendGraphic and GetFeatureInfo operations for user supplied "dynamic styling". Enabling the use of dynamic styles, without also configuring URL checks, provides the opportunity for Service Side Request Forgery. This vulnerability can be used to steal user NetNTLMv2 hashes which could be relayed or cracked externally to gain further access. This vulnerability has been patched in versions 2.22.5 and 2.23.2.	2023-10-25	not yet calculated	CVE-2023-41339 MISC <https://github.com/geoserver/geoserver/security/advisories/ghsa-cqpc-x2c6-2gmf> MISC <https://github.com/geoserver/geoserver/releases/tag/2.22.5> MISC <https://github.com/geoserver/geoserver/releases/tag/2.23.2>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The OGC Web Processing Service (WPS) specification is designed to process information from any server using GET and POST requests. This presents the opportunity for Server Side Request Forgery. This vulnerability has been patched in version 2.22.5 and 2.23.2.	2023-10-25	not yet calculated	CVE-2023-43795 MISC <https://github.com/geoserver/geoserver/security/advisories/ghsa-5pr3-m5hm-9956>
geoserver -- geowebcache	A vulnerability was found in GeoServer GeoWebCache up to 1.15.1. It has been declared as problematic. This vulnerability affects unknown code of the file /geoserver/gwc/rest.html. The manipulation leads to direct request. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243592.	2023-10-26	not yet calculated	CVE-2023-5786 MISC MISC MISC <https://github.com/qxyday/geoserve---unauthorized>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
github -- enterprise_server	Incorrect Permission Assignment for Critical Resource in GitHub Enterprise Server that allowed local operating system user accounts to read MySQL connection details including the MySQL password via configuration files. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.7.18, 3.8.11, 3.9.6, and 3.10.3.	2023-10-25	not yet calculated	CVE-2023-23767 MISC <https://docs.github.com/en/enterprise-server@3.9/admin/release-notes#3.9.6> MISC <https://docs.github.com/en/enterprise-server@3.8/admin/release-notes#3.8.11> MISC <https://docs.github.com/en/enterprise-server@3.

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				7/admin/release-notes#3.7.18> MISC <https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.3>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onTaskAppeared of PipTaskOrganizer.java, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40116 MISC <https://android.googlesource.com/platform/frameworks/base/+/18c3b194642f3949d09e48c21da5658fa04994c8> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40117 MISC <https://android.googlesource.com/platform/frameworks/base/+/ff86ff28cf82124f8e65833a2dd8c319aea08945> MISC <https://android.googlesource.com/platform/packages/apps/settings/+/11815817de2f2d70fe842b108356a1bc75d44ffb> MISC <https://s

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ource.android.com/security/bulletin/2023-10-01>
google -- android	In multiple locations, there is a possible way to bypass user notification of foreground services due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40120 MISC <https://android.googlesource.com/platform/frameworks/base/+/d26544e5a4fd554b790b4d0c5964d9e95d9e626b> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In appendEscapedSQLString of DatabaseUtils.java, there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40121 MISC <https://android.googlesource.com/platform/frameworks/base/+/3287ac2d2565dc96bf6177967f8e3aed33954253> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40123 MISC <https://android.googlesource.com/platform/frameworks/base/+/7212a4bec2d2f1a74fa54a12a04255d6a183baa9> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40125 MISC <https://android.googlesource.com/platform/packages/apps/settings/+/63d464c3fa5c7b9900448fef3844790756e557eb> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40127 MISC <https://android.googlesource.com/platform/packages/providers/mediaprovider/+/7474312506125 07e8289ae8eb1a56303e79ab678> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In several functions of xmlregexp.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40128 MISC <https://android.googlesource.com/platform/external/libxml2/+/1ccf89b87a3969edd56956e2d447f896037c8be7> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In build_read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40129 MISC <https://android.googlesource.com/platform/packages/modules/bluetooth/+/c0151aa3ba76c785b32c7f9d16c98febe53017b1> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40130 MISC <https://android.googlesource.com/platform/packages/services/telecomm/+/5b335401d1c8de7d1c85f4a0cf353f7f9fc30218> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40131 MISC <https://android.googlesource.com/platform/frameworks/native/+/0cda11569dd256ff3220b4fe44f861f8081d7116> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40133 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In isFullScreen of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40134 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40135 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40136 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40137 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40138 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40139 MISC <https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In android_view_InputDevice_create of android_view_InputDevice.cpp, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	not yet calculated	CVE-2023-40140 MISC <https://android.googlesource.com/platform/frameworks/base/+/2d88a5c481df8986dbba2e02c5bf82f105b36243> MISC <https://source.android.com/security/bulletin/2023-10-01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-10-25	not yet calculated	CVE-2023-5472 MISC <https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_24.html> MISC <https://crbug.com/1491296> MISC <https://www.debian.org/security/2023/dsa-5536> MISC <https://lists.fedoraproject.org/archives/list/pack

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				age-announce@lists.fedoraproject.org/message/tdmqg42vvoz5ussi4nsnt3vjpgbpnsiw/>
gougucms -- gougucms	gougucms v4.08.18 was discovered to contain a password reset poisoning vulnerability which allows attackers to arbitrarily reset users' passwords via a crafted packet.	2023-10-27	not yet calculated	CVE-2023-46393 MISC <https://gitee.com/gouguopen/gougucms/issues/i88tkh>
gougucms -- gougucms	A stored cross-site scripting (XSS) vulnerability in /home/user/edit_submit of gougucms v4.08.18 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the headimgurl parameter.	2023-10-27	not yet calculated	CVE-2023-46394 MISC <https://gitee.com/gouguopen/gougucms/issues/i88tc0>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
grafana -- grafana	Grafana is an open-source platform for monitoring and observability. The WorldMap panel plugin, versions before 1.0.4 contains a DOM XSS vulnerability.	2023-10-25	not yet calculated	CVE-2023-3010 MISC <https://grafana.com/security/security-advisories/cve-2023-3010/>
hashicorp -- vagrant	HashiCorp Vagrant's Windows installer targeted a custom location with a non-protected path that could be junctioned, introducing potential for unauthorized file system writes. Fixed in Vagrant 2.4.0.	2023-10-27	not yet calculated	CVE-2023-5834 MISC <https://discuss.hashicorp.com/t/hcsec-2023-31-vagrant-s-windows-installer-allowed-directory-junction-write/59568>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hcl_software -- hcl_commerce	HCL Commerce Remote Store server could allow a remote attacker, using a specially-crafted URL, to read arbitrary files on the system.	2023-10-23	not yet calculated	CVE-2023-37532 MISC
hewlett_packard_enterprise -- aruba_clearpass_policy_manager	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance.	2023-10-25	not yet calculated	CVE-2023-43506 MISC <https://www.arubanetworks.com/assets/alert/aruba-psa-2023-016.txt>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hewlett_packard_enterprise -- aruba_clearpass_policy_manager	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster.	2023-10-25	not yet calculated	CVE-2023-43507 MISC <https://www.arubanetworks.com/assets/alert/aruba-psa-2023-016.txt>
hewlett_packard_enterprise -- aruba_clearpass_policy_manager	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform.	2023-10-25	not yet calculated	CVE-2023-43508 MISC <https://www.arubanetworks.com/assets/alert/aruba-psa-2023-016.txt>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hewlett_packard_enterprise -- aruba_clearpass_policy_manager	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software.	2023-10-25	not yet calculated	CVE-2023-43509 MISC <https://www.arubanetworks.com/assets/alert/aruba-psa-2023-016.txt>
hewlett_packard_enterprise -- aruba_clearpass_policy_manager	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise.	2023-10-25	not yet calculated	CVE-2023-43510 MISC <https://www.arubanetworks.com/assets/alert/aruba-psa-2023-016.txt>
hewlett_packard_enterprise -- hpe_oneview	A remote code execution issue exists in HPE OneView.	2023-10-25	not yet calculated	CVE-2023-30912 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp_inc. -- hp_print_and_scan_doctor_for_windows	HP Print and Scan Doctor for Windows may potentially be vulnerable to escalation of privilege. HP is releasing software updates to mitigate the potential vulnerability.	2023-10-25	not yet calculated	CVE-2023-5671 MISC <https://support.hp.com/us-en/document/ish_9502679-9502704-16>
hu60wap6 -- hu60wap6	A vulnerability classified as problematic was found in hu60t hu60wap6. Affected by this vulnerability is the function markdown of the file src/class/ubbparser.php. The manipulation leads to cross site scripting. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named a1cd9f12d7687243bfcb7ce295665acb83b9174e. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-243775.	2023-10-28	not yet calculated	CVE-2023-5835 MISC <https://github.com/hu60t/hu60wap6/commit/a1cd9f12d7687243bfcb7ce295665acb83b9174e> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- txseries_for_multiplatforms	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016.	2023-10-25	not yet calculated	CVE-2023-42031 MISC <https://www.ibm.com/support/pages/node/7056429> MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/266061> MISC <https://www.ibm.com/support/pages/node/7056433>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server_liberty	IBM WebSphere Application Server Liberty 23.0.0.9 through 23.0.0.10 could provide weaker than expected security due to improper resource expiration handling. IBM X-Force ID: 268775.	2023-10-25	not yet calculated	CVE-2023-46158 MISC <https://www.ibm.com/support/pages/node/7058356> MISC <https://exchange.xforce.ibmcloud.com/vulnerabilities/268775>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
icecms -- icecms	IceCMS v2.0.1 is vulnerable to Cross Site Request Forgery (CSRF).	2023-10-27	not yet calculated	CVE-2023-42188 MISC <https://topdayplus.github.io/2023/10/27/cve-deatail/> MISC <https://github.com/thecosy/icecms/issues/17>
idattend_pty_ltd -- idweb	Reflected cross-site scripting in the StudentSearch component in IDAttend's IDWeb application 3.1.052 and earlier allows hijacking of a user's browsing session by attackers who have convinced the said user to click on a malicious link.	2023-10-25	not yet calculated	CVE-2023-1356 MISC <https://www.themissinglink.com.au/security-advisories/cve-2023-1356>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ilias -- ilias	ILIAS (2013-09-12 release) contains a medium-criticality Directory Traversal local file inclusion vulnerability in the ScormAicc module. An attacker with a privileged account, typically holding the tutor role, can exploit this to gain unauthorized access to and potentially retrieve confidential files stored on the web server. The attacker can access files that are readable by the web server user www-data; this may include sensitive configuration files and documents located outside the documentRoot. The vulnerability is exploited by an attacker who manipulates the file parameter in a URL, inserting directory traversal sequences in order to access unauthorized files. This manipulation allows the attacker to retrieve sensitive files, such as /etc/passwd, potentially compromising the system's security. This issue poses a significant risk to confidentiality and is remotely exploitable over the internet.	2023-10-26	not yet calculated	CVE-2023-45867 MISC <https://rehmeinfosec.de> MISC <https://rehmeinfosec.de/labor/cve-2023-45867>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ilias -- ilias	The Learning Module in ILIAS 7.25 (2023-09-12 release) allows an attacker (with basic user privileges) to achieve a high-impact Directory Traversal attack on confidentiality and availability. By exploiting this network-based vulnerability, the attacker can move specified directories, normally outside the documentRoot, to a publicly accessible location via the PHP function rename(). This results in a total loss of confidentiality, exposing sensitive resources, and potentially denying access to the affected component and the operating system's components. To exploit this, an attacker must manipulate a POST request during the creation of an exercise unit, by modifying the old_name and new_name parameters via directory traversal. However, it's essential to note that, when exploiting this vulnerability, the specified directory will be relocated from its original location, rendering all files obtained from there unavailable.	2023-10-26	not yet calculated	CVE-2023-45868 MISC <https://rehmeinfosec.de> MISC <https://rehmeinfosec.de/labor/cve-2023-45867>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ilias -- ilias	ILIAS 7.25 (2023-09-12) allows any authenticated user to execute arbitrary operating system commands remotely, when a highly privileged account accesses an XSS payload. The injected commands are executed via the exec() function in the execQuoted() method of the ilUtil class (/Services/Utilities/classes/class.ilUtil.php) This allows attackers to inject malicious commands into the system, potentially compromising the integrity, confidentiality, and availability of the ILIAS installation and the underlying operating system.	2023-10-26	not yet calculated	CVE-2023-45869 MISC <https://rehmeinfosec.de/labor/cve-2023-45869> MISC <https://rehmeinfosec.de/report/358ad5f6-f712-4f74-a5ee-476efc856cbc/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ispconfig -- ispconfig	An issue was discovered in ISPConfig before 3.2.11p1. PHP code injection can be achieved in the language file editor by an admin if admin_allow_langedit is enabled.	2023-10-27	not yet calculated	CVE-2023-46818 MISC <https://www.ispconfig.org/blog/ispconfig-3-2-11p1-released/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iterm2 -- iterm2	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of certain escape sequences related to tmux integration.	2023-10-22	not yet calculated	CVE-2023-46300 MISC <https://github.com/gnachman/iterm2/commit/b2268b03b5f3d4cd8ca275eaef5d16d0fac20009> MISC <https://blog.solidsnail.com/posts/2023-08-28-iterm2-rce> MISC <https://iterm2.com/news.html> MISC <https://github.com/gnachman/iterm2/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				commit/ae8192522661c34d1cbe57f6f9ef2ff0a337c2a5>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iterm2 -- iterm2	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of certain escape sequences related to upload.	2023-10-22	not yet calculated	CVE-2023-46301 MISC <https://github.com/gnachman/iterm2/commit/b2268b03b5f3d4cd8ca275eaef5d16d0fac20009> MISC <https://blog.solidsnail.com/posts/2023-08-28-iterm2-rce> MISC <https://iterm2.com/news.html> MISC <https://github.com/gnachman/iterm2/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				commit/85cbf5ebda472c9ec295887e99c2b6f1b5867f1b>
iterm2 -- iterm2	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize paths in x-man-page URLs. They may have shell metacharacters for a /usr/bin/man command line.	2023-10-23	not yet calculated	CVE-2023-46321 MISC <https://iterm2.com/downloads.html> MISC <https://gitlab.com/gnachman/iterm2/-/commit/de3d351e1bd3bc1c1a4f85fe976c592e497dd071>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iterm2 -- iterm2	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize ssh hostnames in URLs. The hostname's initial character may be non-alphanumeric. The hostname's other characters may be outside the set of alphanumeric characters, dash, and period.	2023-10-23	not yet calculated	CVE-2023-46322 MISC <https://iterm2.com/downloads.html> MISC <https://gitlab.com/gnachman/iterm2/-/commit/ef7bb84520013b2524df9787d4aa9f2c96746c01>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itop -- itop	iTop is an open source, web-based IT service management platform. Prior to versions 3.0.4 and 3.1.0, when displaying `pages/preferences.php`, cross site scripting is possible. This issue is fixed in versions 3.0.4 and 3.1.0.	2023-10-25	not yet calculated	CVE-2023-34446 MISC <https://github.com/combodo/itop/security/advisories/ghsa-q4pp-j46r-gm68> MISC <https://github.com/combodo/itop/commit/e3ba826e5dfd3b724f1ee97bebfd20ded3c70b10>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itop -- itop	iTop is an open source, web-based IT service management platform. Prior to versions 3.0.4 and 3.1.0, on `pages/UI.php`, cross site scripting is possible. This issue is fixed in versions 3.0.4 and 3.1.0.	2023-10-25	not yet calculated	CVE-2023-34447 MISC <https://github.com/combodo/itop/commit/519751faa10b2fc5b75ea4516a1b8ef13ca35b33> MISC <https://github.com/combodo/itop/commit/b8f61362f570e1ef8127175331012b7fc8aba802> MISC <https://github.com/combodo/itop/security/advisories/ghsa-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				6rfm-2rwg-mj7p>
ivanti -- secure_access_client	A logged in user may elevate its permissions by abusing a Time-of-Check to Time-of-Use (TOCTOU) race condition. When a particular process flow is initiated, an attacker can exploit this condition to gain unauthorized elevated privileges on the affected system.	2023-10-25	not yet calculated	CVE-2023-38041 MISC
jenkins -- jenkins	Jenkins GitHub Plugin 1.37.3 and earlier does not escape the GitHub project URL on the build page when showing changes, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2023-10-25	not yet calculated	CVE-2023-46650 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3246>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins Warnings Plugin 10.5.0 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to. This fix has been backported to 10.4.1.	2023-10-25	not yet calculated	CVE-2023-46651 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3265>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins --jenkins	A missing permission check in Jenkins lambdatest-automation Plugin 1.20.9 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of LAMBDATEST credentials stored in Jenkins.	2023-10-25	not yet calculated	CVE-2023-46652 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3222>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins lambdatest-automation Plugin 1.20.10 and earlier logs LAMBDATEST Credentials access token at the INFO level, potentially resulting in its exposure.	2023-10-25	not yet calculated	CVE-2023-46653 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3202>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the expected directory during the cleanup process of the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to delete arbitrary files on the Jenkins controller file system.	2023-10-25	not yet calculated	CVE-2023-46654 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3237>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the directory from which artifacts are published during the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to publish arbitrary files from the Jenkins controller file system to the previously configured CloudBees CD server.	2023-10-25	not yet calculated	CVE-2023-46655 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3238>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins Multibranch Scan Webhook Trigger Plugin 1.0.9 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	not yet calculated	CVE-2023-46656 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-2875>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins Gogs Plugin 1.0.15 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	not yet calculated	CVE-2023-46657 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-2896>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins MSTeams Webhook Trigger Plugin 0.1.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	not yet calculated	CVE-2023-46658 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-2876>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins Edgewall Trac Plugin 1.13 and earlier does not escape the Trac website URL on the build page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2023-10-25	not yet calculated	CVE-2023-46659 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-3247>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins Zanata Plugin 0.6 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token hashes are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	not yet calculated	CVE-2023-46660 MISC <http://www.openwall.com/lists/oss-security/2023/10/25/2> MISC <https://www.jenkins.io/security/advisory/2023-10-25/#security-2879>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jose4j -- jose4j	jose4j before v0.9.3 allows attackers to set a low iteration count of 1000 or less.	2023-10-25	not yet calculated	CVE-2023-31582 MISC <https://bitbucket.org/b_c/jose4j/issues/203/insecure-support-of-setting-pbe-less-then> MISC <https://github.com/kanixb/jwtissues/blob/main/jose4j%20issue.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jumpserver -- jumpserver	jumpserver is an open source bastion machine, professional operation and maintenance security audit system that complies with 4A specifications. A flaw in the Core API allows attackers to bypass password brute-force protections by spoofing arbitrary IP addresses. By exploiting this vulnerability, attackers can effectively make unlimited password attempts by altering their apparent IP address for each request. This vulnerability has been patched in version 3.8.0.	2023-10-25	not yet calculated	CVE-2023-46123 MISC <https://github.com/jumpserver/jumpserver/security/advisories/ghsa-hvw4-766m-p89f> MISC <https://github.com/jumpserver/jumpserver/releases/tag/v3.8.0>
juzawebcms -- juzawebcms	Cross Site Scripting vulnerability in juzawebCMS v.3.4 and before allows a remote attacker to execute arbitrary code via a crafted payload to the username parameter of the registration page.	2023-10-28	not yet calculated	CVE-2023-46467 MISC <https://www.sumor.top/index.php/archives/872/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juzawebcms -- juzawebcms	An issue in juzawebCMS v.3.4 and before allows a remote attacker to execute arbitrary code via a crafted file to the custom plugin function.	2023-10-28	not yet calculated	CVE-2023-46468 MISC <https://www.sumor.top/index.php/archives/875/>
knot_resolver -- knot_resolver	Knot Resolver before 5.7.0 performs many TCP reconnections upon receiving certain nonsensical responses from servers.	2023-10-22	not yet calculated	CVE-2023-46317 MISC <https://gitlab.nic.cz/knot/knot-resolver/-/merge_requests/1448> MISC <https://www.knot-resolver.cz/2023-08-22-knot-resolver-5.7.0.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kodbox -- kodbox	kodbox 1.44 is vulnerable to Cross Site Scripting (XSS). Customizing global HTML results in storing XSS.	2023-10-23	not yet calculated	CVE-2023-45998 MISC <https://gist.github.com/fangjiuye/703fdb643db558640f23e4e7c9532348>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kubernetes -- ingress-nginx	Ingress-nginx `path` sanitization can be bypassed with `log_format` directive.	2023-10-25	not yet calculated	CVE-2022-4886 MISC <https://github.com/kubernetes/ingress-nginx/issues/10570> MISC <https://groups.google.com/g/kubernetes-security-announce/c/ge7u3qcwzli> MISC <http://www.openwall.com/lists/oss-security/2023/10/25/5>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kubernetes -- ingress-nginx	Ingress nginx annotation injection causes arbitrary command execution.	2023-10-25	not yet calculated	CVE-2023-5043 MISC <https://github.com/kubernetes/ingress-nginx/issues/10571> MISC <https://groups.google.com/g/kubernetes-security-announce/c/pvsxsopxyzo> MISC <http://www.openwall.com/lists/oss-security/2023/10/25/4>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kubernetes -- ingress-nginx	Code injection via nginx.ingress.kubernetes.io/permanent-redirect annotation.	2023-10-25	not yet calculated	CVE-2023-5044 MISC <https://github.com/kubernetes/ingress-nginx/issues/10572> MISC <https://groups.google.com/g/kubernetes-security-announce/c/ukuyyvrnel0> MISC <http://www.openwall.com/lists/oss-security/2023/10/25/3>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- app_store	An information disclosure vulnerability has been identified in the Lenovo App Store which may allow some applications to gain unauthorized access to sensitive user data used by other unrelated applications.	2023-10-27	not yet calculated	CVE-2022-3611 MISC <https://iknow.lenovo.com.cn/detail/205280.html>
lenovo -- elliptic_labs_virtual_lock_sensor	A vulnerability was reported in Elliptic Labs Virtual Lock Sensor for ThinkPad T14 Gen 3 that could allow an attacker with local access to execute code with elevated privileges.	2023-10-25	not yet calculated	CVE-2023-3112 MISC <https://support.lenovo.com/us/en/product_security/len-128081>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- hardwarescanplugin	A denial of service vulnerability was reported in the Lenovo HardwareScanPlugin versions prior to 1.3.1.2 and Lenovo Diagnostics versions prior to 4.45 that could allow a local user with administrative access to trigger a system crash.	2023-10-25	not yet calculated	CVE-2022-0353 MISC <https://support.lenovo.com/us/en/product_security/len-102365> MISC <https://support.lenovo.com/us/en/product_security/len-94532>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- hardwarescanplugin	A denial of service vulnerability was reported in the Lenovo HardwareScanPlugin versions prior to 1.3.1.2 and Lenovo Diagnostics versions prior to 4.45 that could allow a local user with administrative access to trigger a system crash.	2023-10-25	not yet calculated	CVE-2022-3698 MISC <https://support.lenovo.com/us/en/product_security/len-102365> MISC <https://support.lenovo.com/us/en/product_security/len-94532>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- hardwarescanplugin	A privilege escalation vulnerability was reported in the Lenovo HardwareScanPlugin prior to version 1.3.1.2 and Lenovo Diagnostics prior to version 4.45 that could allow a local user to execute code with elevated privileges.	2023-10-25	not yet calculated	CVE-2022-3699 MISC <https://support.lenovo.com/us/en/product_security/len-102365> MISC <https://support.lenovo.com/us/en/product_security/len-94532>
lenovo -- hardwarescanplugin	A denial of service vulnerability was reported in Lenovo Vantage HardwareScan Plugin version 1.3.0.5 and earlier that could allow a local attacker to delete contents of an arbitrary directory under certain conditions.	2023-10-27	not yet calculated	CVE-2022-3702 MISC <https://support.lenovo.com/us/en/product_security/len-94532>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- printer_gm265dn	A denial-of-service vulnerability was found in the firmware used in Lenovo printers, where users send illegal or malformed strings to an open port, triggering a denial of service that causes a display error and prevents the printer from functioning properly.	2023-10-27	not yet calculated	CVE-2022-3429 MISC <https://iknow.lenovo.com.cn/detail/205041.html>
lenovo -- printer_gm265dn	A remote code execution vulnerability was found in the firmware used in some Lenovo printers, which can be caused by a remote user pushing an illegal string to the server-side interface via a script, resulting in a stack overflow.	2023-10-27	not yet calculated	CVE-2022-34886 MISC <https://iknow.lenovo.com.cn/detail/205041.html>
lenovo -- printer_gm265dn	Standard users can directly operate and set printer configuration information , such as IP, in some Lenovo Printers without having to authenticate with the administrator password.	2023-10-27	not yet calculated	CVE-2022-34887 MISC <https://iknow.lenovo.com.cn/detail/205041.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- thinksystem	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	2023-10-25	not yet calculated	CVE-2023-4606 MISC <https://support.lenovo.com/us/en/product_security/len-140960>
lenovo -- thinksystem	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	2023-10-25	not yet calculated	CVE-2023-4608 MISC <https://support.lenovo.com/us/en/product_security/len-140960>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- vantage_systemupdate_plugin	A Time of Check Time of Use (TOCTOU) vulnerability was reported in the Lenovo Vantage SystemUpdate Plugin version 2.0.0.212 and earlier that could allow a local attacker to delete arbitrary files.	2023-10-27	not yet calculated	CVE-2022-3700 MISC <https://support.lenovo.com/us/en/product_security/len-94532>
lenovo -- vantage_systemupdate_plugin	A privilege elevation vulnerability was reported in the Lenovo Vantage SystemUpdate plugin version 2.0.0.212 and earlier that could allow a local attacker to execute arbitrary code with elevated privileges.	2023-10-27	not yet calculated	CVE-2022-3701 MISC <https://support.lenovo.com/us/en/product_security/len-94532>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
light-oauth2 -- light-oauth2	light-oauth2 before version 2.1.27 obtains the public key without any verification. This could allow attackers to authenticate to the application with a crafted JWT token.	2023-10-25	not yet calculated	CVE-2023-31580 MISC <https://github.com/networknt/light-oauth2/issues/369> MISC <https://github.com/kanixb/jwtissues/blob/main/certification%20verification%20issue%20in%20light-oauth2.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- kernel	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware guest with 3D acceleration enabled, a local, unprivileged user could potentially use this flaw to escalate their privileges.	2023-10-23	not yet calculated	CVE-2023-5633 MISC <https://access.redhat.com/security/cve/cve-2023-5633> MISC
linux -- kernel	An issue was discovered in the Linux kernel before 6.5.9, exploitable by local users with userspace access to MMIO registers. Incorrect access checking in the #VC handler and instruction emulation of the SEV-ES emulation of MMIO accesses could lead to arbitrary write access to kernel memory (and thus privilege escalation). This depends on a race condition through which userspace can replace an instruction before the #VC handler reads it.	2023-10-27	not yet calculated	CVE-2023-46813 MISC <https://cdn.kernel.org/pub/linux/kernel/v6.x/changelog-6.5.9> MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- kernel	A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation. If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06.	2023-10-25	not yet calculated	CVE-2023-5717 MISC <https://kernel.dance/32671e3799ca2e4590773fd0e63aaa4229e50c06> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
man-group -- dtale	D-Tale is the combination of a Flask back-end and a React front-end to view & analyze Pandas data structures. Prior to version 3.7.0, users hosting D-Tale publicly can be vulnerable to remote code execution, allowing attackers to run malicious code on the server. This issue has been patched in version 3.7.0 by turning off "Custom Filter" input by default. The only workaround for versions earlier than 3.7.0 is to only host D-Tale to trusted users.	2023-10-25	not yet calculated	CVE-2023-46134 MISC <https://github.com/man-group/dtale/security/advisories/ghsa-jq6c-r9xf-qxjm> MISC <https://github.com/man-group/dtale/commit/bf8c54ab2490803f45f0652a9a0e221a94d39668>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
marbre_lapin_line -- marbre_lapin_line	An issue in Marbre Lapin Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	2023-10-25	not yet calculated	CVE-2023-38846 MISC <https://liff.line.me/1657925980-kmmgkje5> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-38846.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
matsuya_line -- matsuya_line	The leakage of the client secret in Matsuya Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39737 MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39737.md> MISC <https://liff.line.me/1657535522-jd5q5yp1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
matter-labs -- era-compiler-vyper	era-compiler-vyper is the EraVM Vyper compiler for zkSync Era, a layer 2 rollup that uses zero-knowledge proofs to scale Ethereum. Prior to era-compiler-vype version 1.3.10, a bug prevented the initialization of the first immutable variable for Vyper contracts meeting certain criteria. The problem arises when there is a String or Array with more 256-bit words allocated than initialized. It results in the second word's index unset, that is effectively set to 0, so the first immutable value with the actual 0 index is overwritten in the ImmutableSimulator. Version 1.3.10 fixes this issue by setting all indexes in advance. The problem will go away, but it will get more expensive if the user allocates a lot of uninitialized space, e.g. `String[4096]`. Upgrading and redeploying affected contracts is the only way of working around the issue.	2023-10-25	not yet calculated	CVE-2023-46232 MISC <https://github.com/matter-labs/era-compiler-vyper/commit/8be305a1b9c68d0fd47dad3434224ed85944ca25> MISC <https://github.com/matter-labs/era-compiler-vyper/security/advisories/ghsa-h8jv-969m-94r4> MISC <https://github.com/matter-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				labs/era-system-contracts/blob/main/contracts/immutablesimulator.sol#l37>
memcached -- memcached	In Memcached before 1.6.22, a buffer overflow exists when processing multiget requests in proxy mode, if there are many spaces after the "get" substring.	2023-10-27	not yet calculated	CVE-2023-46852 MISC <https://github.com/memcached/memcached/commit/76a6c363c18cfe7b6a1524ae64202ac9db330767> MISC <https://github.com/memcached/memcached/compare/1.6.21...1.6.22>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
memcached -- memcached	In Memcached before 1.6.22, an off-by-one error exists when processing proxy requests in proxy mode, if \n is used instead of \r\n.	2023-10-27	not yet calculated	CVE-2023-46853 MISC <https://github.com/memcached/memcached/compare/1.6.21...1.6.22> MISC <https://github.com/memcached/memcached/commit/6987918e9a3094ec4fc8976f01f769f624d790fa>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mercury_a15 -- mercury_a15	Mercury A15 V1.0 20230818_1.0.3 was discovered to contain a command execution vulnerability via the component cloudDeviceTokenSuccCB.	2023-10-25	not yet calculated	CVE-2023-46518 MISC <https://service.mercurycom.com.cn/download-2341.html> MISC <https://github.com/xyiym/digging/blob/main/mercury/a15/1/1.md> MISC <https://www.mercurycom.com.cn/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mintty -- mintty	An issue in Mintty v.3.6.4 and before allows a remote attacker to execute arbitrary code via crafted commands to the terminal.	2023-10-26	not yet calculated	CVE-2023-39726 MISC <https://dgl.cx/2023/09/ansi-terminal-security#mintty-osc50>
motorola -- mr2600_router	A vulnerability has been identified in the MR2600 router v1.0.18 and earlier that could allow an attacker within range of the wireless network to successfully brute force the WPS pin, potentially allowing them unauthorized access to a wireless network.	2023-10-27	not yet calculated	CVE-2022-3681 MISC <https://web.archive.org/web/20230317174952/https://help.motorolanetwork.com/hc/en-us/articles/9933302506523>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	Using iterative requests an attacker was able to learn the size of an opaque response, as well as the contents of a server-supplied Vary header. This vulnerability affects Firefox < 119.	2023-10-25	not yet calculated	CVE-2023-5722 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC
mozilla -- firefox	An attacker with temporary script access to a site could have set a cookie containing invalid characters using `document.cookie` that could have led to unknown errors. This vulnerability affects Firefox < 119.	2023-10-25	not yet calculated	CVE-2023-5723 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	A malicious web site can enter fullscreen mode while simultaneously triggering a WebAuthn prompt. This could have obscured the fullscreen notification and could have been leveraged in a spoofing attack. This vulnerability affects Firefox < 119.	2023-10-25	not yet calculated	CVE-2023-5729 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC
mozilla -- firefox	Memory safety bugs present in Firefox 118. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119.	2023-10-25	not yet calculated	CVE-2023-5731 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox_for_ios	When opening a page in reader mode, the redirect URL could have caused attacker-controlled script to execute in a reflected Cross-Site Scripting (XSS) attack. This vulnerability affects Firefox for iOS < 119.	2023-10-25	not yet calculated	CVE-2023-5758 MISC <https://www.mozilla.org/security/advisories/mfsa2023-48/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5721 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC MISC <https://www.debian.org/sec

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				urity/2023/dsa-5535> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00037.html> MISC <https://www.debian.org/security/2023/dsa-5538> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00042.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5724 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC MISC <https://www.debian.org/sec

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				urity/2023/dsa-5535> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00037.html> MISC <https://www.debian.org/security/2023/dsa-5538> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00042.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5725 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC <https://www.debian.org/sec

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				urity/2023/dsa-5535> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00037.html> MISC <https://www.debian.org/security/2023/dsa-5538> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00042.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. *Note: This issue only affected macOS operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5726 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	The executable file warning was not presented when downloading .msix, .msixbundle, .appx, and .appxbundle files, which can run commands on a user's computer. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5727 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	During garbage collection extra operations were performed on a object that should not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5728 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC MISC <https://www.debian.org/sec

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				urity/2023/dsa-5535> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00037.html> MISC <https://www.debian.org/security/2023/dsa-5538> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00042.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5730 MISC <https://www.mozilla.org/security/advisories/mfsa2023-45/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC MISC <https://www.debian.org/sec

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				urity/2023/dsa-5535> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00037.html> MISC <https://www.debian.org/security/2023/dsa-5538> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00042.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- multiple_products	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	not yet calculated	CVE-2023-5732 MISC <https://www.mozilla.org/security/advisories/mfsa2023-34/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-47/> MISC <https://www.mozilla.org/security/advisories/mfsa2023-46/> MISC MISC MISC <https://www.debia

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				n.org/security/2023/dsa-5535> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00037.html> MISC <https://www.debian.org/security/2023/dsa-5538> MISC <https://lists.debian.org/debian-lts-announce/2023/10/msg00042.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nanning_ontall_software_co._ltd. -- longxing_industrial_development_zone_project_construction_and_installation_management_system	A vulnerability was found in Nanning Ontall Longxing Industrial Development Zone Project Construction and Installation Management System up to 20231026. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.aspx. The manipulation of the argument tbxUserName leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243727.	2023-10-27	not yet calculated	CVE-2023-5828 MISC MISC MISC <https://github.com/echosssy/-sql-injection/blob/main/%e5%8d%97%e5%ae%81%e5%b8%82%e5%ae%89%e6%8b%93%e8%bd%af%e4%bb%b6%e6%9c%89%e9%99%90%e5%85%ac%e5%8f%b8sql%20injection.doc>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nautobot -- nautobot	Nautobot is a Network Automation Platform built as a web application atop the Django Python framework with a PostgreSQL or MySQL database. In Nautobot 2.0.x, certain REST API endpoints, in combination with the `?depth=<N>` query parameter, can expose hashed user passwords as stored in the database to any authenticated user with access to these endpoints. The passwords are not exposed in plaintext. This vulnerability has been patched in version 2.0.3.	2023-10-25	not yet calculated	CVE-2023-46128 MISC <https://github.com/nautobot/nautobot/security/advisories/ghsa-r2hw-74xv-4gqp> MISC <https://github.com/nautobot/nautobot/pull/4692> MISC <https://github.com/nautobot/nautobot/commit/1ce8e5c658a075c29554d517cd453675e5d40d71>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netentsec -- ns-asg_application_security_gateway	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /protocol/firewall/uploadfirewall.php. The manipulation of the argument messagecontent leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243590 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-26	not yet calculated	CVE-2023-5784 MISC MISC MISC <https://github.com/gb111d/ns-asg_poc/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netentsec -- ns-asg_application_security_gateway	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file /protocol/firewall/addaddress_interpret.php. The manipulation of the argument messagecontent leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243591. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-26	not yet calculated	CVE-2023-5785 MISC MISC MISC <https://github.com/ggg48966/cve/blob/main/ns-asg-sql-addaddress_interpret.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netentsec -- ns-asg_application_security_gateway	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/list_onlineuser.php. The manipulation of the argument SessionId leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243716. NOTE: We tried to contact the vendor early about the disclosure, but the official mail address was not working properly.	2023-10-27	not yet calculated	CVE-2023-5826 MISC MISC <https://github.com/cubi123123123/cve/blob/main/ns-asg-sql-list_onlineuser.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netmodule -- router_software	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105.	2023-10-22	not yet calculated	CVE-2023-46306 MISC <https://share.netmodule.com/public/system-software/4.8/4.8.0.101/nrsw-rn-4.8.0.101.pdf> MISC <https://share.netmodule.com/public/system-software/4.6/4.6.0.106/nrsw-rn-4.6.0.106.pdf> MISC <https://pentest.blog/advisory-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				netmodule-router-software-race-condition-leads-to-remote-code-execution/>
nextgen_healthcare -- mirth_connect	NextGen Healthcare Mirth Connect before version 4.4.1 is vulnerable to unauthenticated remote code execution. Note that this vulnerability is caused by the incomplete patch of CVE-2023-37679.	2023-10-26	not yet calculated	CVE-2023-43208 MISC <https://www.horizon3.ai/nextgen-mirth-connect-remote-code-execution-vulnerability-cve-2023-43208/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
npmjs -- npmjs_node_email_check	ReDos in NPMJS Node Email Check v.1.0.4 allows an attacker to cause a denial of service via a crafted string to the scpSyntax component.	2023-10-25	not yet calculated	CVE-2023-39619 MISC <https://gist.github.com/6en6ar/712a4c1eab0324f15e09232c77ea08f8> MISC <https://www.npmjs.com/package/node-email-check> MISC <https://github.com/teomantuncer/node-email-check/blob/main/main.js,>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
obl.ong -- obl.ong	The admin panel for Obl.ong before 1.1.2 allows authorization bypass because the email OTP feature accepts arbitrary numerical values.	2023-10-26	not yet calculated	CVE-2023-46754 MISC <https://github.com/obl-ong/admin/releases/tag/v1.1.2>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ocomon -- ocomon	An information disclosure vulnerability in the component users-grid-data.php of Ocomon before v4.0.1 allows attackers to obtain sensitive information such as e-mails and usernames.	2023-10-26	not yet calculated	CVE-2023-33558 MISC <https://github.com/ninj4c0d3r/ocomon-research> MISC <https://github.com/ninj4c0d3r/ocomon-research/commit/6357def478b11119270b89329fceb115f12c69fc>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ocomon -- ocomon	A local file inclusion vulnerability via the lang parameter in OcoMon before v4.0.1 allows attackers to execute arbitrary code by supplying a crafted PHP file.	2023-10-26	not yet calculated	CVE-2023-33559 MISC <https://github.com/ninj4c0d3r/ocomon-research/commit/7459ff397f48b5356930c16c522331e39158461dv> MISC <https://github.com/ninj4c0d3r/ocomon-research>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
omron_corporation -- cx-designer	CX-Designer Ver.3.740 and earlier (included in CX-One CXONE-AL[][]D-V4) contains an improper restriction of XML external entity reference (XXE) vulnerability. If a user opens a specially crafted project file created by an attacker, sensitive information in the file system where CX-Designer is installed may be disclosed.	2023-10-23	not yet calculated	CVE-2023-43624 MISC <https://jvn.jp/en/vu/jvnvu98683567/> MISC <https://www.fa.omron.co.jp/product/security/assets/pdf/en/omsr-2023-011_en.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
onigiriya-musubee_line -- onigiriya-musubee_line	The leakage of the client secret in Onigiriya-musubee Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39740 MISC <https://liff.line.me/1657597257-0ozj8dwj> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39740.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openssl -- openssl	Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths. This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers. Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the "keylen" parameter or the IV length, via the "ivlen" parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for	2023-10-25	not yet calculated	CVE-2023-5363 MISC <https://www.openssl.org/news/secadv/20231024.txt> MISC <http://www.openwall.com/lists/oss-security/2023/10/24/1> MISC MISC MISC <https://www.debian.org/security/2023/dsa-5532> MISC <https://security.netapp.com/advisory/n

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. It is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However, if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this			tap-20231027-0010/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.			
palantir -- palantir	Gotham Orbital-Simulator service prior to 0.692.0 was found to be vulnerable to a Path traversal issue allowing an unauthenticated user to read arbitrary files on the file system.	2023-10-26	not yet calculated	CVE-2023-30967 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pallets -- werkzeug	Werkzeug is a comprehensive WSGI web application library. If an upload of a file that starts with CR or LF and then is followed by megabytes of data without these characters: all of these bytes are appended chunk by chunk into internal bytearray and lookup for boundary is performed on growing buffer. This allows an attacker to cause a denial of service by sending crafted multipart data to an endpoint that will parse it. The amount of CPU time required can block worker processes from handling legitimate requests. This vulnerability has been patched in version 3.0.1.	2023-10-25	not yet calculated	CVE-2023-46136 MISC <https://github.com/pallets/werkzeug/commit/f3c803b3ade485a45f12b6d6617595350c0f03e2> MISC <https://github.com/pallets/werkzeug/security/advisories/ghsa-hrfv-mqp8-q5rw>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parse_server -- parse_server	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server crashes when uploading a file without extension. This vulnerability has been patched in versions 5.5.6 and 6.3.1.	2023-10-25	not yet calculated	CVE-2023-46119 MISC <https://github.com/parse-community/parse-server/security/advisories/ghsa-792q-q67h-w579> MISC <https://github.com/parse-community/parse-server/releases/tag/6.3.1> MISC <https://github.com/parse-community/parse-server/releases/tag

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				/5.5.6> MISC <https://github.com/parse-community/parse-server/commit/686a9f282dc23c31beab3d93e6d21ccd0e1328fe> MISC <https://github.com/parse-community/parse-server/commit/fd86278919556d3682e7e2c856dfccd5beffbfc0>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pfsense_ce -- pfsense_ce	Pfsense CE version 2.6.0 is vulnerable to No rate limit which can lead to an attacker creating multiple malicious users in firewall.	2023-10-25	not yet calculated	CVE-2023-29973 MISC <https://www.esecforte.com/cve-2023-29973-no-rate-limit/>
phpgurukul -- nipah_virus_testing_management_system	Cross-Site Scripting (XSS) vulnerability in PHPGurukul Nipah virus (NiV) " Testing Management System v.1.0 allows attackers to execute arbitrary code via a crafted payload injected into the State field.	2023-10-25	not yet calculated	CVE-2023-46583 MISC <https://github.com/rumble773/sec-research/blob/main/niv/cve-2023-46583.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- nipah_virus_testing_management_system	SQL Injection vulnerability in PHPGurukul Nipah virus (NiV) " Testing Management System v.1.0 allows a remote attacker to escalate privileges via a crafted request to the new-user-testing.php endpoint.	2023-10-25	not yet calculated	CVE-2023-46584 MISC <https://github.com/rumble773/sec-research/blob/main/niv/cve-2023-46584.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- nipah_virus_testing_management_system	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The identifier VDB-243617 was assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5804 MISC MISC MISC <https://github.com/jacksonstonee/nipah-virus-niv-testing-management-system-using-php-and-mysql-1.0-has-a-sql-injection-vuln-login.php/blob/main/readme.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- online_railway_catering_system	A vulnerability was found in PHPGurukul Online Railway Catering System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-243600.	2023-10-26	not yet calculated	CVE-2023-5794 MISC <https://github.com/jacksonstonee/online-railway-catering-system-1.0-has-a-sql-injection-vulnerability-in-index.php/tree/main> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ping_identity -- pingfederate	When an AWS DynamoDB table is used for user attribute storage, it is possible to retrieve the attributes of another user using a maliciously crafted request.	2023-10-25	not yet calculated	CVE-2023-34085 MISC <https://docs.pingidentity.com/r/en-us/pingfederate-113/gyk1689105783244> MISC <https://www.pingidentity.com/en/resources/downloads/pingfederate.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ping_identity -- pingfederate	Under a very specific and highly unrecommended configuration, authentication bypass is possible in the PingFederate Identifier First Adapter	2023-10-25	not yet calculated	CVE-2023-37283 MISC <https://docs.pingidentity.com/r/en-us/pingfederate-113/gyk1689105783244> MISC <https://www.pingidentity.com/en/resources/downloads/pingfederate.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ping_identity -- pingfederate	PingFederate Administrative Console dependency contains a weakness where console becomes unresponsive with crafted Java class loading enumeration requests	2023-10-25	not yet calculated	CVE-2023-39219 MISC <https://docs.pingidentity.com/r/en-us/pingfederate-113/gyk1689105783244> MISC <https://www.pingidentity.com/en/resources/downloads/pingfederate.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ping_identity -- pingfederate	PingFederate using the PingOne MFA adapter allows a new MFA device to be paired without requiring second factor authentication from an existing registered device. A threat actor may be able to exploit this vulnerability to register their own MFA device if they have knowledge of a victim user's first factor credentials.	2023-10-25	not yet calculated	CVE-2023-39231 MISC <https://docs.pingidentity.com/r/en-us/pingfederate-pingone-mfa-ik/bks16573031943 94> MISC <https://www.pingidentity.com/en/resources/downloads/pingid.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ping_identity -- pingfederate	A first-factor authentication bypass vulnerability exists in the PingFederate with PingID Radius PCV when a MSCHAP authentication request is sent via a maliciously crafted RADIUS client request.	2023-10-25	not yet calculated	CVE-2023-39930 MISC <https://docs.pingidentity.com/r/en-us/pingid/pingid_integration_kit_2_26_rn> MISC <https://www.pingidentity.com/en/resources/downloads/pingfederate.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pip -- pip	When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the "hg clone" call (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren't installing from Mercurial.	2023-10-25	not yet calculated	CVE-2023-5752 MISC <https://mail.python.org/archives/list/security-announce@python.org/thread/f4pl35u6x4vvhz5ilju3pwuwn7h7lzxl/> MISC <https://github.com/pypa/pip/pull/12306>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prestashop -- prestashop	In the module "Product Catalog (CSV, Excel, XML) Export PRO" (exportproducts) in versions up to 4.1.1 from MyPrestaModules for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack. Due to a lack of permissions control and a lack of control in the path name construction, a guest can perform a path traversal to view all files on the information system.	2023-10-25	not yet calculated	CVE-2023-46346 MISC <https://security.friendsofpresta.org/modules/2023/10/24/exportproducts.html>
prestashop -- prestashop	In the module "Step by Step products Pack" (ndk_steppingpack) version 1.5.6 and before from NDK Design for PrestaShop, a guest can perform SQL injection. The method `NdkSpack::getPacks()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	2023-10-25	not yet calculated	CVE-2023-46347 MISC <https://security.friendsofpresta.org/modules/2023/10/24/ndk_steppingpack.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prestashop -- prestashop	In the module "Referral and Affiliation Program" (referralbyphone) version 3.5.1 and before from Snegurka for PrestaShop, a guest can perform SQL injection. Method `ReferralByPhoneDefaultModuleFrontController::ajaxProcessCartRuleValidate` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	2023-10-25	not yet calculated	CVE-2023-46358 MISC <https://security.friendsofpresta.org/modules/2023/10/24/referralbyphone.html>
proxmox -- proxmox	Proxmox proxmox-widget-toolkit before 4.0.9, as used in multiple Proxmox products, allows XSS via the edit notes feature.	2023-10-28	not yet calculated	CVE-2023-46854 MISC MISC MISC <https://pve.proxmox.com/wiki/package_repositories#sysadmin_test_repo>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rabbitmq -- rabbitmq	RabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it vulnerable for denial of service (DoS) attacks with very large messages. An authenticated user with sufficient credentials can publish a very large messages over the HTTP API and cause target node to be terminated by an "out-of-memory killer"-like mechanism. This vulnerability has been patched in versions 3.11.24 and 3.12.7.	2023-10-25	not yet calculated	CVE-2023-46118 MISC <https://github.com/rabbitmq/rabbitmq-server/security/advisories/ghsa-w6cq-9cf4-gqpg>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rabbitmq -- rabbitmq	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ nodes. `maxBodyLebgth` was not used when receiving Message objects. Attackers could send a very large Message causing a memory overflow and triggering an OOM Error. Users of RabbitMQ may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. This vulnerability was patched in version 5.18.0.	2023-10-25	not yet calculated	CVE-2023-46120 MISC <https://github.com/rabbitmq/rabbitmq-java-client/releases/tag/v5.18.0> MISC <https://github.com/rabbitmq/rabbitmq-java-client/issues/1062> MISC <https://github.com/rabbitmq/rabbitmq-java-client/security/advisories/ghsa-mm8h-8587-p46h>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC <https://github.com/rabbitmq/rabbitmq-java-client/commit/714aae602dcae6cb4b53cadf009323ebac313cc8>
radare2 -- radare2	An out-of-bounds read in radare2 v.5.8.9 and before exists in the print_insn32_fpu function of libr/arch/p/nds32/nds32-dis.h.	2023-10-28	not yet calculated	CVE-2023-46569 MISC <https://github.com/radareorg/radare2/issues/22334> MISC <https://gist.github.com/gandalf4a/afeaf8cc958f95876f0ee245b8a002e8>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
radare2 -- radare2	An out-of-bounds read in radare2 v.5.8.9 and before exists in the print_insn32 function of libr/arch/p/nds32/nds32-dis.h.	2023-10-28	not yet calculated	CVE-2023-46570 MISC <https://gist.github.com/gandalf4a/d7fa58f1b3418ef08ad244acccc10ba6> MISC <https://github.com/radareorg/radare2/issues/22333>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
regina_sweets&bakery_line -- regina_sweets&bakery_line	The leakage of the client secret in REGINA SWEETS&BAKERY Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39739 MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39739.md> MISC <https://liff.line.me/1656985266-emlxqqqx>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
remark42 -- remark42	umputun remark42 version 1.12.1 and before has a Blind Server-Side Request Forgery (SSRF) vulnerability.	2023-10-23	not yet calculated	CVE-2023-45966 MISC <https://github.com/jet-pentest/cve-2023-45966> MISC <https://github.com/umputun/remark42/issues/1677>
rexroth -- ctrlx_hmi_web_panel	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network.	2023-10-25	not yet calculated	CVE-2023-41255 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rexroth -- ctrlx_hmi_web_panel	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself.	2023-10-25	not yet calculated	CVE-2023-41960 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>
rexroth -- ctrlx_hmi_web_panel	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB.	2023-10-25	not yet calculated	CVE-2023-43488 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rexroth -- ctrlx_hmi_web_panel	The Android Client application, when enrolled with the define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user.	2023-10-25	not yet calculated	CVE-2023-45220 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>
rexroth -- ctrlx_hmi_web_panel	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug).	2023-10-25	not yet calculated	CVE-2023-45844 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rexroth -- ctrlx_hmi_web_panel	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker-controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair	2023-10-25	not yet calculated	CVE-2023-41372 MISC <https://psirt.bosch.com/security-advisories/bosch-sa-175607.html>
ritecms -- ritecms	A File upload vulnerability in RiteCMS 3.0 allows a local attacker to upload a SVG file with XSS content.	2023-10-25	not yet calculated	CVE-2023-44767 MISC <https://github.com/sromanhu/ritecms-file-upload--xss---filemanager/blob/main/readme.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rmc_r_beauty_clinic_line -- rmc_r_beauty_clinic_line	An issue in rmc R Beauty CLINIC Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	2023-10-25	not yet calculated	CVE-2023-38848 MISC <https://liff.line.me/1657640647-wk2xyj38> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-38848.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rockwell_automation -- arena_simulation	An arbitrary code execution vulnerability was reported to Rockwell Automation in Arena Simulation that could potentially allow a malicious user to commit unauthorized arbitrary code to the software by using a memory buffer overflow. The threat-actor could then execute malicious code on the system affecting the confidentiality, integrity, and availability of the product. The user would need to open a malicious file provided to them by the attacker for the code to execute.	2023-10-27	not yet calculated	CVE-2023-27854 MISC <https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141145>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rockwell_automation -- arena_simulation	Rockwell Automation Arena Simulation contains an arbitrary code execution vulnerability that could potentially allow a malicious user to commit unauthorized code to the software by using an uninitialized pointer in the application. The threat-actor could then execute malicious code on the system affecting the confidentiality, integrity, and availability of the product. The user would need to open a malicious file provided to them by the attacker for the code to execute.	2023-10-27	not yet calculated	CVE-2023-27858 MISC <https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141145>
rockwell_automation -- factorytalk	Rockwell Automation FactoryTalk View Site Edition insufficiently validates user input, which could potentially allow threat actors to send malicious data bringing the product offline. If exploited, the product would become unavailable and require a restart to recover resulting in a denial-of-service condition.	2023-10-27	not yet calculated	CVE-2023-46289 MISC <https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141167>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rockwell_automation -- factorytalk	Due to inadequate code logic, a previously unauthenticated threat actor could potentially obtain a local Windows OS user token through the FactoryTalk® Services Platform web service and then use the token to log in into FactoryTalk® Services Platform . This vulnerability can only be exploited if the authorized user did not previously log in into the FactoryTalk® Services Platform web service.	2023-10-27	not yet calculated	CVE-2023-46290 MISC <https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141165>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samba -- samba	A heap-based Buffer Overflow flaw was discovered in Samba. It could allow a remote, authenticated attacker to exploit this vulnerability to cause a denial of service.	2023-10-25	not yet calculated	CVE-2023-5568 MISC <https://access.redhat.com/security/cve/cve-2023-5568> MISC MISC MISC <https://www.samba.org/samba/history/samba-4.19.2.html>
satoken -- satoken	An issue in Dromara SaToken version 1.3.50RC and before when using Spring dynamic controllers, a specially crafted request may cause an authentication bypass.	2023-10-25	not yet calculated	CVE-2023-43961 MISC <https://github.com/dromara/sa-token/issues/511>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
satoken -- satoken	An issue in Dromara SaToken version 1.36.0 and before allows a remote attacker to escalate privileges via a crafted payload to the URL.	2023-10-25	not yet calculated	CVE-2023-44794 MISC <https://github.com/dromara/sa-token/issues/515>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sbt -- sbt	sbt is a build tool for Scala, Java, and others. Given a specially crafted zip or JAR file, `IO.unzip` allows writing of arbitrary file. This would have potential to overwrite `/root/.ssh/authorized_keys`. Within sbt's main code, `IO.unzip` is used in `pullRemoteCache` task and `Resolvers.remote`; however many projects use `IO.unzip(...)` directly to implement custom tasks. This vulnerability has been patched in version 1.9.7.	2023-10-23	not yet calculated	CVE-2023-46122 MISC <https://github.com/sbt/io/issues/358> MISC <https://github.com/sbt/sbt/security/advisories/ghsa-h9mw-grgx-2fhf> MISC <https://github.com/sbt/io/commit/124538348db0713c80793cb57b915f97ec13188a> MISC <https://github.com/sbt/io/pull/360>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sd-webui-infinite-image-browsing -- sd-webui-infinite-image-browsing	The zanllp sd-webui-infinite-image-browsing (aka Infinite Image Browsing) extension before 977815a for stable-diffusion-webui (aka Stable Diffusion web UI), if Gradio authentication is enabled without secret key configuration, allows remote attackers to read any local file via /file?path= in the URL, as demonstrated by reading /proc/self/environ to discover credentials.	2023-10-22	not yet calculated	CVE-2023-46315 MISC <https://github.com/zanllp/sd-webui-infinite-image-browsing/pull/368/commits/977815a2b28ad953c10ef0114c365f698c4b8f19> MISC <https://github.com/zanllp/sd-webui-infinite-image-browsing/issues/387>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
seacms -- seacms	An issue in SeaCMS v.12.9 allows an attacker to execute arbitrary commands via the admin_safe.php component.	2023-10-25	not yet calculated	CVE-2023-46010 MISC MISC <http://seacms.com>
shaanxi_chanming_education_technology -- score_query_system	A vulnerability was found in Shaanxi Chanming Education Technology Score Query System 5.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument stuldCard leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243593 was assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5787 MISC MISC MISC <https://github.com/echosssy/-sql-injection-exists-in-the-score-query-system/blob/main/readme.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
shanghai_cti_navigation -- cti_monitoring_and_early_warning_system	A vulnerability was found in Shanghai CTI Navigation CTI Monitoring and Early Warning System 2.2. It has been classified as critical. This affects an unknown part of the file /Web/SysManage/UserEdit.aspx. The manipulation of the argument ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-243717 was assigned to this vulnerability.	2023-10-27	not yet calculated	CVE-2023-5827 MISC MISC MISC <https://github.com/ox1dq/cve/blob/main/rce.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sick_ag -- fx0-gmod00000	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay.	2023-10-23	not yet calculated	CVE-2023-5246 MISC <https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf> MISC <https://sick.com/psirt> MISC <https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco -- analog_fm_transmitter	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter.	2023-10-26	not yet calculated	CVE-2023-41966 MISC <https://www.sielco.org/en/contacts> MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-08>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco -- analog_fm_transmitter	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter.	2023-10-26	not yet calculated	CVE-2023-42769 MISC <https://www.sielco.org/en/contacts> MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-08>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco -- analog_fm_transmitter	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters.	2023-10-26	not yet calculated	CVE-2023-45228 MISC <https://www.sielco.org/en/contacts> MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-08>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco -- analog_fm_transmitter	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	2023-10-26	not yet calculated	CVE-2023-45317 MISC <https://www.sielco.org/en/contacts> MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-08>
sielco_ -- polyeco1000	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests.	2023-10-26	not yet calculated	CVE-2023-46661 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco_ -- polyeco1000	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information.	2023-10-26	not yet calculated	CVE-2023-46662 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>
sielco_ -- polyeco1000	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests.	2023-10-26	not yet calculated	CVE-2023-46663 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco_ -- polyeco1000	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages.	2023-10-26	not yet calculated	CVE-2023-46664 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>
sielco_ -- polyeco1000	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges.	2023-10-26	not yet calculated	CVE-2023-46665 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sielco_ -- polyeco1000	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system.	2023-10-26	not yet calculated	CVE-2023-5754 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>
sielco_ -- polyeco1000	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests.	2023-10-26	not yet calculated	CVE-2023-0897 MISC <https://www.cisa.gov/news-events/ics-advisories/icsa-23-299-07>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
silicon_labs -- ember_znet_sdk	Missing Encryption of Security Keys vulnerability in Silicon Labs Ember ZNet SDK on 32 bit, ARM (SecureVault High modules) allows potential modification or extraction of network credentials stored in flash. This issue affects Silicon Labs Ember ZNet SDK: 7.3.1 and earlier.	2023-10-26	not yet calculated	CVE-2023-41096 MISC
silicon_labs -- openthread_sdk	Missing Encryption of Security Keys vulnerability in Silicon Labs OpenThread SDK on 32 bit, ARM (SecureVault High modules) allows potential modification or extraction of network credentials stored in flash. This issue affects Silicon Labs OpenThread SDK: 2.3.1 and earlier.	2023-10-26	not yet calculated	CVE-2023-41095 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sisqualwfm -- sisqualwfm	The sisqualWFM 7.1.319.103 thru 7.1.319.111 for Android, has a host header injection vulnerability in its "/sisqualIdentityServer/core/" endpoint. By modifying the HTTP Host header, an attacker can change webpage links and even redirect users to arbitrary or malicious locations. This can lead to phishing attacks, malware distribution, and unauthorized access to sensitive resources.	2023-10-25	not yet calculated	CVE-2023-36085 MISC <https://github.com/omershaik0/handmade_exploits/tree/main/sisqualwfm-host-header-injection-cve-2023-36085>
sonicwall -- directory_services_connector	A local privilege escalation vulnerability in SonicWall Directory Services Connector Windows MSI client 4.1.21 and earlier versions allows a local low-privileged user to gain system privileges through running the recovery feature.	2023-10-27	not yet calculated	CVE-2023-44219 MISC <https://psirt.global.sonicwall.com/vuln-detail/snwlid-2023-0016>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sonicwall -- netextender_windows	SonicWall NetExtender Windows (32-bit and 64-bit) client 10.2.336 and earlier versions have a DLL Search Order Hijacking vulnerability in the start-up DLL component. Successful exploitation via a local attacker could result in command execution in the target system.	2023-10-27	not yet calculated	CVE-2023-44220 MISC <https://psirt.global.sonicwall.com/vuln-detail/snwlid-2023-0017>
sourcecodester -- file_manager_app	A vulnerability classified as critical was found in SourceCodester File Manager App 1.0. Affected by this vulnerability is an unknown functionality of the file endpoint/add-file.php. The manipulation of the argument uploadedFileName leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243595.	2023-10-26	not yet calculated	CVE-2023-5790 MISC MISC MISC <https://github.com/yp1oneer/cve_hub/blob/main/file%20manager%20app/unrestricted%20file%20upload.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- free_and_open_source_inventory_management_system	Sourcecodester Free and Open Source inventory management system v1.0 is vulnerable to Incorrect Access Control. An arbitrary user can change the password of another user and takeover the account via IDOR in the password change function.	2023-10-26	not yet calculated	CVE-2023-46449 MISC MISC <https://github.com/sajaljat/cve-2023-46449/tree/main>
sourcecodester -- free_and_open_source_inventory_management_system	Sourcecodester Free and Open Source inventory management system 1.0 is vulnerable to Cross Site Scripting (XSS) via the Add supplier function.	2023-10-26	not yet calculated	CVE-2023-46450 MISC <https://youtu.be/lqy0_xik2q0> MISC <https://github.com/yte121/-cve-2023-46450/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- simple_real_estate_portal_system	A vulnerability was found in SourceCodester Simple Real Estate Portal System 1.0. It has been classified as critical. Affected is an unknown function of the file view_estate.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-243618 is the identifier assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5805 MISC MISC MISC <https://github.com/lxxcute/bug/blob/main/real%20estate%20portal%20system%20view_estate.php%20has%20sqlinjection.pdf>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- sticky_notes_app	A vulnerability, which was classified as problematic, was found in SourceCodester Sticky Notes App 1.0. This affects an unknown part of the file endpoint/add-note.php. The manipulation of the argument noteTitle/noteContent leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243597 was assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5791 MISC <https://github.com/yp1oneer/cve_hub/blob/main/sticky%20notes%20app/cross%20site%20scripting.pdf> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- sticky_notes_app	A vulnerability has been found in SourceCodester Sticky Notes App 1.0 and classified as critical. This vulnerability affects unknown code of the file endpoint/delete-note.php. The manipulation of the argument note leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243598 is the identifier assigned to this vulnerability.	2023-10-26	not yet calculated	CVE-2023-5792 MISC <https://github.com/yp1oneer/cve_hub/blob/main/sticky%20notes%20app/sql%20injection-1.pdf> MISC MISC
sourcecodester -- task_reminder_system	A vulnerability was found in SourceCodester Task Reminder System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=delete_reminder. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-243644.	2023-10-27	not yet calculated	CVE-2023-5813 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- task_reminder_system	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been classified as critical. This affects an unknown part of the file /classes/Master.php?f=save_reminder. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-243645 was assigned to this vulnerability.	2023-10-27	not yet calculated	CVE-2023-5814 MISC MISC
sourcecodester -- task_reminder_system	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file classes/Users.php?f=delete. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-243800.	2023-10-28	not yet calculated	CVE-2023-5836 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- packers_and_movers_management_system	Sourcecodester Packers and Movers Management System v1.0 is vulnerable to SQL Injection via mpms/?p=services/view_service&id.	2023-10-26	not yet calculated	CVE-2023-46435 MISC <https://github.com/kirra-max/bug_reports/blob/main/packers-and-movers-management-system-phpoop-free-source-code/sql-1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stb_image.h -- stb_image.h	Double Free vulnerability in Nothings Stb Image.h v.2.28 allows a remote attacker to cause a denial of service via a crafted file to the stbi_load_gif_main function.	2023-10-25	not yet calculated	CVE-2023-43281 MISC <https://gist.github.com/peccc/d8761f6ac45ad55cbd194dd7e6fdfdac> MISC <https://github.com/peccc/double-stb>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stellar -- rs-stellar-strkey	rs-stellar-strkey is a Rust lib for encode/decode of Stellar Strkeys. A panic vulnerability occurs when a specially crafted payload is used.`inner_payload_len` should not above 64. This vulnerability has been patched in version 0.0.8.	2023-10-25	not yet calculated	CVE-2023-46135 MISC <https://github.com/stellar/rs-stellar-strkey/issues/58> MISC <https://github.com/stellar/rs-stellar-strkey/security/advisories/ghsa-5873-6fwq-463f>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sugarcrm -- sugarcrm	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. An Unrestricted File Upload vulnerability has been identified in the Notes module. By using a crafted request, custom PHP code can be injected via the Notes module because of missing input validation. An attacker with regular user privileges can exploit this.	2023-10-27	not yet calculated	CVE-2023-46815 MISC <https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-011/>
sugarcrm -- sugarcrm	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. A Server Site Template Injection (SSTI) vulnerability has been identified in the GecControl action. By using a crafted request, custom PHP code can be injected via the GetControl action because of missing input validation. An attacker with regular user privileges can exploit this.	2023-10-27	not yet calculated	CVE-2023-46816 MISC <https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-010/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synology -- camera_firmware	A vulnerability regarding use of externally controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be affected: BC500 and TC500.	2023-10-25	not yet calculated	CVE-2023-5746 MISC <https://www.synology.com/en-global/security/advisory/synology_sa_23_11>
tenable -- nessus_network_monitor	Under certain conditions, Nessus Network Monitor could allow a low privileged user to escalate privileges to NT AUTHORITY\SYSTEM on Windows hosts by replacing a specially crafted file.	2023-10-26	not yet calculated	CVE-2023-5622 MISC <https://www.tenable.com/security/tns-2023-34>
tenable -- nessus_network_monitor	NNM failed to properly set ACLs on its installation directory, which could allow a low privileged user to run arbitrary code with SYSTEM privileges where NNM is installed to a non-standard location	2023-10-26	not yet calculated	CVE-2023-5623 MISC <https://www.tenable.com/security/tns-2023-34>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- nessus_network_monitor	Under certain conditions, Nessus Network Monitor was found to not properly enforce input validation. This could allow an admin user to alter parameters that could potentially allow a blindSQL injection.	2023-10-26	not yet calculated	CVE-2023-5624 MISC <https://www.tenable.com/security/tns-2023-34>
tenda -- w18e	Tenda W18E V16.01.0.8(1576) contains a stack overflow vulnerability via the portMirrorMirroredPorts parameter in the formSetNetCheckTools function.	2023-10-25	not yet calculated	CVE-2023-46369 MISC <https://github.com/archerber/bug_submit/blob/main/tenda/w18e/bug1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- w18e	Tenda W18E V16.01.0.8(1576) has a command injection vulnerability via the hostName parameter in the formSetNetCheckTools function.	2023-10-25	not yet calculated	CVE-2023-46370 MISC <https://github.com/archerber/bug_submit/blob/main/tenda/w18e/bug2.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tibco_software_inc. -- tibco_hawk	The Hawk Console and Hawk Agent components of TIBCO Software Inc.'s TIBCO Hawk, TIBCO Hawk Distribution for TIBCO Silver Fabric, TIBCO Operational Intelligence Hawk RedTail, and TIBCO Runtime Agent contain a vulnerability that theoretically allows an attacker with access to the Hawk Console's and Agent's log to obtain credentials used to access associated EMS servers. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.2.2 and below, TIBCO Hawk Distribution for TIBCO Silver Fabric: versions 6.2.2 and below, TIBCO Operational Intelligence Hawk RedTail: versions 7.2.1 and below, and TIBCO Runtime Agent: versions 5.12.2 and below.	2023-10-25	not yet calculated	CVE-2023-26219 MISC <https://www.tibco.com/services/support/advisories>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tire-sales_line -- tire-sales_line	An issue in tire-sales Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request.	2023-10-25	not yet calculated	CVE-2023-38849 MISC <https://liff.line.me/1657203739-yvgg5pjn> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-38849.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tokueimaru_waiting_line -- ztokueimaru_waiting_line	The leakage of the client secret in Tokueimaru_waiting Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39732 MISC <https://liff.line.me/1657574837-elb6bnqj> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39732.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tongda --oa	A vulnerability classified as critical was found in Tongda OA 2017 11.10. This vulnerability affects unknown code of the file general/system/approve_center/flow_guide/flow_type/set_print/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243586 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-26	not yet calculated	CVE-2023-5780 MISC MISC MISC <https://github.com/rceraser/cve/blob/main/sql_inject_5.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tongda --oa	A vulnerability, which was classified as critical, has been found in Tongda OA 2017 11.10. This issue affects the function DELETE_STR of the file general/system/res_manage/monitor/delete_webmail.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243587. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-26	not yet calculated	CVE-2023-5781 MISC <https://github.com/wangxinyudad/cve/blob/main/sql.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tongda --oa	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.10. Affected is an unknown function of the file /manage/delete_query.php of the component General News. The manipulation of the argument NEWS_ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243588. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-26	not yet calculated	CVE-2023-5782 MISC <https://github.com/charmeeeeee/tongda-oa-repo/blob/main/tongda_oa_vulnerability_report.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tongda --oa	A vulnerability has been found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/system/approve_center/flow_sort/flow/delete.php. The manipulation of the argument id/sort_parent leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243589 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-26	not yet calculated	CVE-2023-5783 MISC <https://github.com/halleyakina/cve/blob/main/sql.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tonton-tei_line -- tonton-tei_line	The leakage of the client secret in TonTon-Tei Line v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39733 MISC <https://liff.line.me/1656987103-bk5k9po4> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39733.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formNtp.	2023-10-25	not yet calculated	CVE-2023-46540 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/11/1.md> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formIpv6Setup.	2023-10-25	not yet calculated	CVE-2023-46541 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/10/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMeshUploadConfig.	2023-10-25	not yet calculated	CVE-2023-46542 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/13/1.md> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWlSiteSurvey.	2023-10-25	not yet calculated	CVE-2023-46543 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/16/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWirelessTbl.	2023-10-25	not yet calculated	CVE-2023-46544 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/14/1.md>
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWsc.	2023-10-25	not yet calculated	CVE-2023-46545 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/17/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formStats.	2023-10-25	not yet calculated	CVE-2023-46546 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/15/1.md> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formSysLog.	2023-10-25	not yet calculated	CVE-2023-46547 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/12/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formWlanRedirect.	2023-10-25	not yet calculated	CVE-2023-46548 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/1/1.md>
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formSetLg.	2023-10-25	not yet calculated	CVE-2023-46549 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/18/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMapDelDevice.	2023-10-25	not yet calculated	CVE-2023-46550 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/21/1.md#2firmware-download-address> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formReflashClientTbl.	2023-10-25	not yet calculated	CVE-2023-46551 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/2/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formMultiAP.	2023-10-25	not yet calculated	CVE-2023-46552 MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/19/1.md> MISC
totolink -- x2000r_firmware	TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formParentControl.	2023-10-25	not yet calculated	CVE-2023-46553 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x2000r/5/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 41DD80 function.	2023-10-25	not yet calculated	CVE-2023-46408 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/16/1.md> MISC
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ 41CC04 function.	2023-10-25	not yet calculated	CVE-2023-46409 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/13/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 416F60 function.	2023-10-25	not yet calculated	CVE-2023-46410 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/10/1.md> MISC
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_415258 function.	2023-10-25	not yet calculated	CVE-2023-46411 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/11/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_41D998 function.	2023-10-25	not yet calculated	CVE-2023-46412 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/15/1.md> MISC
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_4155DC function.	2023-10-25	not yet calculated	CVE-2023-46413 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/1/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ 41D494 function.	2023-10-25	not yet calculated	CVE-2023-46414 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/14/1.md> MISC
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41E588 function.	2023-10-25	not yet calculated	CVE-2023-46415 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/17/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ The 41A414 function.	2023-10-25	not yet calculated	CVE-2023-46416 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/12/1.md>
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415498 function.	2023-10-25	not yet calculated	CVE-2023-46417 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/2/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_412688 function.	2023-10-25	not yet calculated	CVE-2023-46418 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/7/1.md> MISC
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415730 function.	2023-10-25	not yet calculated	CVE-2023-46419 MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/6/1.md> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41590C function.	2023-10-25	not yet calculated	CVE-2023-46420 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/5/1.md>
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411D00 function.	2023-10-25	not yet calculated	CVE-2023-46421 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/8/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411994 function.	2023-10-25	not yet calculated	CVE-2023-46422 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/9/1.md>
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_417094 function.	2023-10-25	not yet calculated	CVE-2023-46423 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/4/1.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- x6000r_firmware	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_422BD4 function.	2023-10-25	not yet calculated	CVE-2023-46424 MISC MISC <https://github.com/xyiym/digging/blob/main/totolink/x6000r/3/1.md>
tp-link -- tl-wdr7660	TP-Link device TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function upgradeInfoJsonToBin.	2023-10-25	not yet calculated	CVE-2023-46371 MISC <https://github.com/archerber/bug_submit/blob/main/tp-link/tl-wdr7660/2.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tp-link -- tl-wdr7660	TP-Link TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function deviceInfoJsonToBincauses.	2023-10-25	not yet calculated	CVE-2023-46373 MISC <https://github.com/archerber/bug_submit/blob/main/tp-link/tl-wdr7660/3.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
traceroute -- traceroute	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines.	2023-10-25	not yet calculated	CVE-2023-46316 MISC <https://security-tracker.debian.org/tracker/cve-2023-46316> MISC <https://sourceforge.net/projects/traceroute/files/traceroute/traceroute-2.1.3/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
twisted -- twisted	Twisted is an event-based framework for internet applications. Prior to version 23.10.0rc1, when sending multiple HTTP requests in one TCP packet, twisted.web will process the requests asynchronously without guaranteeing the response order. If one of the endpoints is controlled by an attacker, the attacker can delay the response on purpose to manipulate the response of the second request when a victim launched two requests using HTTP pipeline. Version 23.10.0rc1 contains a patch for this issue.	2023-10-25	not yet calculated	CVE-2023-46137 MISC <https://github.com/twisted/twisted/security/advisories/ghsa-xc8x-vp79-p3wm>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ubiquiti -- unifi_network_application	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier, implement device adoption with improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later.	2023-10-25	not yet calculated	CVE-2023-41721 MISC <https://community.ui.com/releases/security-advisory-bulletin-036-036/81367bc9-2a64-4435-95dc-bbe482457615>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ubuntu -- ubuntu_grub2	An out-of-bounds write flaw was found in grub2's NTFS filesystem driver. This issue may allow an attacker to present a specially crafted NTFS filesystem image, leading to grub's heap metadata corruption. In some circumstances, the attack may also corrupt the UEFI firmware heap metadata. As a result, arbitrary code execution and secure boot protection bypass may be achieved.	2023-10-25	not yet calculated	CVE-2023-4692 MISC <https://access.redhat.com/security/cve/cve-2023-4692> MISC MISC <https://dfir.ru/2023/10/03/cve-2023-4692-cve-2023-4693-vulnerabilities-in-the-grub-boot-manager/> MISC <https://lists.gnu.org/archive/html/grub-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				devel/2023-10/msg00028.html> MISC <https://seclists.org/oss-sec/2023/q4/37>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ubuntu -- ubuntu_grub2	An out-of-bounds read flaw was found on grub2's NTFS filesystem driver. This issue may allow a physically present attacker to present a specially crafted NTFS file system image to read arbitrary memory locations. A successful attack allows sensitive data cached in memory or EFI variable values to be leaked, presenting a high Confidentiality risk.	2023-10-25	not yet calculated	CVE-2023-4693 MISC MISC <https://access.redhat.com/security/cve/cve-2023-4693> MISC <https://dfir.ru/2023/10/03/cve-2023-4692-cve-2023-4693-vulnerabilities-in-the-grub-boot-manager/> MISC <https://lists.gnu.org/archive/html/grub-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				devel/2023-10/msg00028.html> MISC <https://seclists.org/oss-sec/2023/q4/37>
univention -- ucs@school	Incorrect LDAP ACLs in ucs-school-ldap-acls-master in UCS@school before 4.4v5-errata allow remote teachers, staff, and school administrators to read LDAP password hashes (sambaNTPassword, krb5Key, sambaPasswordHistory, and pwhistory) via LDAP search requests. For example, a teacher can gain administrator access via an NTLM hash.	2023-10-26	not yet calculated	CVE-2020-17477 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
uomasa_saiji_news_line -- uomasa_saiji_news_line	The leakage of the client secret in Uomasa_Saiji_news Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39735 MISC <https://liff.line.me/1657409177-mkplqo5d> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39735.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
uvdesk_community_skeleton -- uvdesk_community_skeleton	UVDesk Community Skeleton v1.1.1 allows unauthenticated attackers to perform brute force attacks on the login page to gain access to the application.	2023-10-23	not yet calculated	CVE-2023-37635 MISC <https://www.esecforte.com/cve-2023-37635-login-bruteforce/>
uvdesk_community_skeleton -- uvdesk_community_skeleton	A stored cross-site scripting (XSS) vulnerability in UVDesk Community Skeleton v1.1.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Message field when creating a ticket.	2023-10-23	not yet calculated	CVE-2023-37636 MISC <https://www.esecforte.com/cve-2023-37636-stored-cross-site-scripting/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vermeg -- agilereporter	An issue was discovered in VERMEG AgileReporter 21.3. XXE can occur via an XML document to the Analysis component.	2023-10-27	not yet calculated	CVE-2022-34832 MISC <https://crashpark.weebly.com/blog/xxe-in-agilereporter-213-by-vermeg> MISC <https://www.vermeg.com/agile-reporter/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vermeg -- agilereporter	An issue was discovered in VERMEG AgileReporter 21.3. An admin can enter an XSS payload in the Analysis component.	2023-10-27	not yet calculated	CVE-2022-34833 MISC <https://crashpark.weebly.com/blog/1-stored-xss-in-agilereporter-213-by-vermeg> MISC <https://www.vermeg.com/agile-reporter/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vermeg -- agilereporter	An issue was discovered in VERMEG AgileReporter 21.3. Attackers can gain privileges via an XSS payload in an Add Comment action to the Activity log.	2023-10-27	not yet calculated	CVE-2022-34834 MISC <https://www.vermeg.com/agile-reporter/> MISC <https://crashpark.weebly.com/blog/2-stored-xss-in-agilereporter-213-by-vermeg>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
viessmann -- vitogate_300	A vulnerability was found in Viessmann Vitogate 300 up to 2.1.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/. The manipulation leads to direct request. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-10-23	not yet calculated	CVE-2023-5702 MISC <https://github.com/gta12138/vul/blob/main/viessmann/vitogate300_document_unauthorized_access.md> MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vim -- vim	Vim is an improved version of the good old UNIX editor Vi. Heap-use-after-free in memory allocated in the function `ga_grow_inner` in in the file `src/alloc.c` at line 748, which is freed in the file `src/ex_docmd.c` in the function `do_cmdline` at line 1010 and then used again in `src/cmdhist.c` at line 759. When using the `:history` command, it's possible that the provided argument overflows the accepted value. Causing an Integer Overflow and potentially later an use-after-free. This vulnerability has been patched in version 9.0.2068.	2023-10-27	not yet calculated	CVE-2023-46246 MISC <https://github.com/vim/vim/security/advisories/ghsa-q22m-h7m2-9mgm> MISC <https://github.com/vim/vim/commit/9198c1f2b1ddecde22af918541e0de2a32f0f45a>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vinchin -- backup_&_recovery	VinChin Backup & Recovery v5.0.*, v6.0.*, v6.7.*, and v7.0.* was discovered to contain a command injection vulnerability.	2023-10-27	not yet calculated	CVE-2023-45498 MISC <https://blog.leakix.net/2023/10/vinchin-backup-rce-chain/> FULLDISC <http://seclists.org/fulldisclosure/2023/oct/31>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vinchin -- backup_&_recovery	VinChin Backup & Recovery v5.0.*, v6.0.*, v6.7.*, and v7.0.* was discovered to contain hardcoded credentials.	2023-10-27	not yet calculated	CVE-2023-45499 MISC <https://blog.leakix.net/2023/10/vinchin-backup-rce-chain/> FULLDISC <http://seclists.org/fulldisclosure/2023/oct/31>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vision_meat_works_trackdiner10/10_mc_line -- vision_meat_works_trackdiner10/10_mc_line	The leakage of the client secret in VISION MEAT WORKS TrackDiner10/10_mc Line v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	2023-10-25	not yet calculated	CVE-2023-39734 MISC <https://liff.line.me/1660679145-emkgg4rj> MISC <https://github.com/syz913/cve-reports/blob/main/cve-2023-39734.md>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware --open-vm-tools	open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs.	2023-10-27	not yet calculated	CVE-2023-34059 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0024.html> MISC <http://www.openwall.com/lists/oss-security/2023/10/27/2> MISC <http://www.openwall.com/lists/oss-security/2023/10/27/3>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware -- vcenter_server	vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution.	2023-10-25	not yet calculated	CVE-2023-34048 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0023.html>
vmware -- vcenter_server	vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data.	2023-10-25	not yet calculated	CVE-2023-34056 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0023.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware -- vmware_tools	VMware Tools contains a local privilege escalation vulnerability. A malicious actor with local user access to a guest virtual machine may elevate privileges within the virtual machine.	2023-10-27	not yet calculated	CVE-2023-34057 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0024.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware -- vmware_tools	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .	2023-10-27	not yet calculated	CVE-2023-34058 MISC <https://www.vmware.com/security/advisories/vmsa-2023-0024.html> MISC <http://www.openwall.com/lists/oss-security/2023/10/27/1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vue.js -- vue.js_devtools	The Vue.js Devtools extension was found to leak screenshot data back to a malicious web page via the standard `postMessage()` API. By creating a malicious web page with an iFrame targeting a sensitive resource (i.e., a locally accessible file or sensitive website), and registering a listener on the web page, the extension sent messages back to the listener, containing the base64 encoded screenshot data of the sensitive resource.	2023-10-23	not yet calculated	CVE-2023-5718 MISC <https://gist.github.com/calumhutton/bdb97077a66021ed455f87823cd7c7cb>
wabt -- wabt	WebAssembly wabt 1.0.33 has an Out-of-Bound Memory Read in in DataSegment::IsValidRange(), which lead to segmentation fault.	2023-10-23	not yet calculated	CVE-2023-46331 MISC <https://github.com/webassembly/wabt/issues/2310>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wabt -- wabt	WebAssembly wabt 1.0.33 contains an Out-of-Bound Memory Write in DataSegment::Drop(), which lead to segmentation fault.	2023-10-23	not yet calculated	CVE-2023-46332 MISC <https://github.com/webassembly/wabt/issues/2311>
wenwenaicms -- wenwenaicms	Insecure Permissions vulnerability in WenwenaiCMS v.1.0 allows a remote attacker to escalate privileges.	2023-10-25	not yet calculated	CVE-2023-45990 MISC <https://github.com/pwncyn/wenwenai/issues/2>
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Print, PDF, Email by PrintFriendly plugin <= 5.5.1 versions.	2023-10-25	not yet calculated	CVE-2023-25032 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Vark Minimum Purchase for WooCommerce plugin <= 2.0.0.1 versions.	2023-10-26	not yet calculated	CVE-2023-30492 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in TotalPress.Org Custom post types, Custom Fields & more plugin <= 4.0.12 versions.	2023-10-26	not yet calculated	CVE-2023-32116 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alkaweb Eonet Manual User Approve plugin <= 2.1.3 versions.	2023-10-27	not yet calculated	CVE-2023-32738 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mitchell Bennis Simple File List plugin <= 6.1.9 versions.	2023-10-25	not yet calculated	CVE-2023-39924 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Animated Counters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-27	not yet calculated	CVE-2023-5774 MISC MISC MISC <https://plugins.trac.wordpress.org/changeset/2984228/>
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TechnoWich WP ULike - Most Advanced WordPress Marketing Toolkit plugin <= 4.6.8 versions.	2023-10-25	not yet calculated	CVE-2023-45640 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Peter Keung Peter's Custom Anti-Spam plugin <= 3.2.2 versions.	2023-10-25	not yet calculated	CVE-2023-45759 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Martin Gibson WP GoToWebinar plugin <= 14.45 versions.	2023-10-25	not yet calculated	CVE-2023-45832 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in LeadSquared Suite plugin <= 0.7.4 versions.	2023-10-25	not yet calculated	CVE-2023-45833 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Libsyn Libsyn Publisher Hub plugin <= 1.4.4 versions.	2023-10-25	not yet calculated	CVE-2023-45835 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in XYDAC Ultimate Taxonomy Manager plugin <= 2.0 versions.	2023-10-25	not yet calculated	CVE-2023-45837 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in XQueue GmbH Maileon for WordPress plugin <= 2.16.0 versions.	2023-10-25	not yet calculated	CVE-2023-46068 MISC
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Osmansorkar Ajax Archive Calendar plugin <= 2.6.7 versions.	2023-10-25	not yet calculated	CVE-2023-46069 MISC
wordpress -- wordpress	An authenticated XCC user can change permissions for any user through a crafted API command.	2023-10-25	not yet calculated	CVE-2023-4607 MISC <https://support.lenovo.com/us/en/product_security/len-140960>
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Emmanuel GEORJON EG-Attachments plugin <= 2.1.3 versions.	2023-10-25	not yet calculated	CVE-2023-46070 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ClickDatos Protección de Datos RGPD plugin <= 3.1.0 versions.	2023-10-25	not yet calculated	CVE-2023-46071 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Michael Simpson Add Shortcodes Actions And Filters plugin <= 2.0.9 versions.	2023-10-26	not yet calculated	CVE-2023-46072 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Borbis Media FreshMail For WordPress plugin <= 2.3.2 versions.	2023-10-26	not yet calculated	CVE-2023-46074 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wpdevart Contact Form Builder, Contact Widget plugin <= 2.1.6 versions.	2023-10-26	not yet calculated	CVE-2023-46075 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RedNao WooCommerce PDF Invoice Builder, Create invoices, packing slips and more plugin <= 1.2.102 versions.	2023-10-26	not yet calculated	CVE-2023-46076 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Arrow Plugins The Awesome Feed - Custom Feed plugin <= 2.2.5 versions.	2023-10-26	not yet calculated	CVE-2023-46077 MISC
wordpress -- wordpress	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Lavacode Lava Directory Manager plugin <= 1.1.34 versions.	2023-10-26	not yet calculated	CVE-2023-46081 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Wpmet Wp Ultimate Review plugin <= 2.2.4 versions.	2023-10-22	not yet calculated	CVE-2023-46085 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology WP Full Stripe Free plugin <= 1.6.1 versions.	2023-10-26	not yet calculated	CVE-2023-46088 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Lee Le @ Userback Userback plugin <= 1.0.13 versions.	2023-10-22	not yet calculated	CVE-2023-46089 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WebDorado WDSocialWidgets plugin <= 1.0.15 versions.	2023-10-26	not yet calculated	CVE-2023-46090 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bala Krishna, Sergey Yakovlev Category SEO Meta Tags plugin <= 2.5 versions.	2023-10-27	not yet calculated	CVE-2023-46091 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in LionScripts.Com Webmaster Tools plugin <= 2.0 versions.	2023-10-27	not yet calculated	CVE-2023-46093 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Conversios Track Google Analytics 4, Facebook Pixel & Conversions API via Google Tag Manager for WooCommerce plugin <= 6.5.3 versions.	2023-10-26	not yet calculated	CVE-2023-46094 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Chetan Gole Smooth Scroll Links [SSL] plugin <= 1.1.0 versions.	2023-10-22	not yet calculated	CVE-2023-46095 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in WP Military WP Radio plugin <= 3.1.9 versions.	2023-10-25	not yet calculated	CVE-2023-46150 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in AWESOME TOGI Product Category Tree plugin <= 2.5 versions.	2023-10-25	not yet calculated	CVE-2023-46151 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOLF - WordPress Posts Bulk Editor and Manager Professional plugin <= 1.0.7.1 versions.	2023-10-25	not yet calculated	CVE-2023-46152 MISC
wordpress -- wordpress	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in UserFeedback Team User Feedback plugin <= 1.0.9 versions.	2023-10-27	not yet calculated	CVE-2023-46153 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Simple Calendar - Google Calendar Plugin <= 3.2.5 versions.	2023-10-25	not yet calculated	CVE-2023-46189 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Novo-media Novo-Map : your WP posts on custom google maps plugin <= 1.1.2 versions.	2023-10-25	not yet calculated	CVE-2023-46190 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Niels van Renselaar Open Graph Metabox plugin <= 1.4.4 versions.	2023-10-25	not yet calculated	CVE-2023-46191 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Internet Marketing Ninjas Internal Link Building plugin <= 1.2.3 versions.	2023-10-27	not yet calculated	CVE-2023-46192 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Internet Marketing Ninjas Internal Link Building plugin <= 1.2.3 versions.	2023-10-25	not yet calculated	CVE-2023-46193 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Eric Teubert Archivist - Custom Archive Templates plugin <= 1.7.5 versions.	2023-10-27	not yet calculated	CVE-2023-46194 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Scientech It Solution Appointment Calendar plugin <= 2.9.6 versions.	2023-10-25	not yet calculated	CVE-2023-46198 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Triberr plugin <= 4.1.1 versions.	2023-10-27	not yet calculated	CVE-2023-46199 MISC
wordpress -- wordpress	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Stephen Darlington, Wandle Software Limited Smart App Banner plugin <= 1.1.3 versions.	2023-10-27	not yet calculated	CVE-2023-46200 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Jeff Sherk Auto Login New User After Registration plugin <= 1.9.6 versions.	2023-10-25	not yet calculated	CVE-2023-46202 MISC
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Muller Digital Inc. Duplicate Theme plugin <= 0.1.6 versions.	2023-10-25	not yet calculated	CVE-2023-46204 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in StylemixThemes Motors - Car Dealer, Classifieds & Listing plugin <= 1.4.6 versions.	2023-10-27	not yet calculated	CVE-2023-46208 MISC
wordpress -- wordpress	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in G5Theme Grid Plus - Unlimited grid plugin <= 1.3.2 versions.	2023-10-27	not yet calculated	CVE-2023-46209 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Brainstorm Force Ultimate Addons for WPBakery Page Builder plugin <= 3.19.14 versions.	2023-10-27	not yet calculated	CVE-2023-46211 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The CallRail Phone Call Tracking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'callrail_form' shortcode in versions up to, and including, 0.5.2 due to insufficient input sanitization and output escaping on the 'form_id' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-27	not yet calculated	CVE-2023-5051 MISC <https://plugins.trac.wordpress.org/changeset/2982876/callrail-phone-call-tracking#file0> MISC MISC <https://plugins.trac.wordpress.org/browser/callrail-phone-call-tracking/tags/0.5.2/callrail.php#l174>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Advanced Menu Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'advMenu' shortcode in versions up to, and including, 0.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-25	not yet calculated	CVE-2023-5085 MISC MISC
wordpress -- wordpress	The BSK PDF Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'bsk-pdfm-category-dropdown' shortcode in versions up to, and including, 3.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-25	not yet calculated	CVE-2023-5110 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Delete Me plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'plugin_delete_me' shortcode in versions up to, and including, 3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The shortcode is not displayed to administrators, so it cannot be used against administrator users.	2023-10-25	not yet calculated	CVE-2023-5126 MISC MISC <https://plugins.trac.wordpress.org/browser/delete-me/tags/3.0/inc/shortcode.php#l83>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WP Font Awesome plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.7.9 due to insufficient input sanitization and output escaping on 'icon' user supplied attribute. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-25	not yet calculated	CVE-2023-5127 MISC MISC MISC MISC MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WP EXtra plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the register() function in versions up to, and including, 6.2. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify the contents of the .htaccess files located in a site's root directory or /wp-content and /wp-includes folders and achieve remote code execution.	2023-10-25	not yet calculated	CVE-2023-5311 MISC <https://giongfnef.gitbook.io/giongfnef/cve/cve-2023-5311> MISC <https://plugins.trac.wordpress.org/changeset/2977703/wp-extra> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Post Meta Data Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pmdm_wp_change_user_meta and pmdm_wp_change_post_meta functions in versions up to, and including, 1.2.0. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to gain elevated (e.g., administrator) privileges.	2023-10-28	not yet calculated	CVE-2023-5425 MISC <https://plugins.trac.wordpress.org/changeset/2981559/post-meta-data-manager> MISC
wordpress -- wordpress	The Post Meta Data Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pmdm_wp_delete_user_meta, pmdm_wp_delete_term_meta, and pmdm_wp_ajax_delete_meta functions in versions up to, and including, 1.2.0. This makes it possible for unauthenticated attackers to delete user, term, and post meta belonging to arbitrary users.	2023-10-28	not yet calculated	CVE-2023-5426 MISC <https://plugins.trac.wordpress.org/changeset/2981559/post-meta-data-manager> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The AI ChatBot plugin for WordPress is vulnerable to unauthorized use of AJAX actions due to missing capability checks on the corresponding functions in versions up to, and including, 4.8.9 as well as 4.9.2. This makes it possible for unauthenticated attackers to perform some of those actions that were intended for higher privileged users.	2023-10-20	not yet calculated	CVE-2023-5533 MISC MISC
wordpress -- wordpress	The AI ChatBot plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.8.9 and 4.9.2. This is due to missing or incorrect nonce validation on the corresponding functions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-20	not yet calculated	CVE-2023-5534 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The VK Filter Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vk_filter_search' shortcode in all versions up to, and including, 2.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-27	not yet calculated	CVE-2023-5705 MISC MISC <https://plugins.trac.wordpress.org/changeset/2983339/vk-filter-search#file1> MISC <https://plugins.trac.wordpress.org/browser/vk-filter-search/tags/2.3.1/inc/filter-search/package/class-vk-filter-search-shortcode.php#l40>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Live Chat with Facebook Messenger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'messenger' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-25	not yet calculated	CVE-2023-5740 MISC MISC <https://plugins.trac.wordpress.org/browser/wp-facebook-messenger/trunk/frontend/shortcode.php#l22> MISC <https://plugins.trac.wordpress.org/browser/wp-facebook-messenger/trunk/frontend/shortcode.php#l32>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Very Simple Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vsgmap' shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-25	not yet calculated	CVE-2023-5744 MISC MISC MISC <https://plugins.trac.wordpress.org/changeset/2982539/very-simple-google-maps#file1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Reusable Text Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'text-blocks' shortcode in versions up to, and including, 1.5.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-25	not yet calculated	CVE-2023-5745 MISC <https://plugins.trac.wordpress.org/browser/reusable-text-blocks/tags/1.5.3/text-blocks.php#l319> MISC
wordpress -- wordpress	The Assistant WordPress plugin before 1.4.4 does not validate a parameter before making a request to it via wp_remote_get(), which could allow users with a role as low as Editor to perform SSRF attacks	2023-10-26	not yet calculated	CVE-2023-5798 MISC <https://wpscan.com/vulnerability/bbb4c98c-4dd7-421e-9666-98f15acde761>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Cross-Site Request Forgery (CSRF) vulnerability in Mihai Iova WordPress Knowledge base & Documentation Plugin - WP Knowledgebase plugin <= 1.3.4 versions.	2023-10-26	not yet calculated	CVE-2023-5802 MISC
wordpress -- wordpress	The Neon text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's neontext_box shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes (color). This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2023-10-27	not yet calculated	CVE-2023-5817 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the addedit functionality. This makes it possible for unauthenticated attackers to upload arbitrary files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-27	not yet calculated	CVE-2023-5820 MISC MISC MISC <https://wordpress.org/plugins/wp-responsive-slider-with-lightbox>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Thumbnail carousel slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing nonce validation on the deleteselected function. This makes it possible for unauthenticated attackers to delete sliders in bulk via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2023-10-27	not yet calculated	CVE-2023-5821 MISC <https://plugins.trac.wordpress.org/changeset/1263536/wp-responsive-slider-with-lightbox/trunk/wp-responsive-slider-with-lightbox.php> MISC <https://wordpress.org/plugins/wp-responsive-thumbnail-slider> MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
writercms -- writercms	Incorrect access control in writercms v1.1.0 allows attackers to directly obtain backend account passwords via unspecified vectors.	2023-10-26	not yet calculated	CVE-2023-43905 MISC <https://github.com/playful-cr/cve-paddle-/blob/main/cve-2023-43905..md>
xnview_classic -- xnview_classic	Buffer Overflow vulnerability in XnView Classic v.2.51.5 allows a local attacker to execute arbitrary code via a crafted TIF file.	2023-10-27	not yet calculated	CVE-2023-46587 MISC <https://github.com/nasroabd/vulns/tree/main/xnview/2.51.5>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xolo_cms -- xolo_cms	Xolo CMS v0.11 was discovered to contain a reflected cross-site scripting (XSS) vulnerability.	2023-10-26	not yet calculated	CVE-2023-43906 MISC <https://github.com/playful-cr/cve-paddle-/blob/main/cve-2023-43906>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xorg-server -- xorg-server	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service.	2023-10-25	not yet calculated	CVE-2023-5367 MISC MISC <https://access.redhat.com/security/cve/cve-2023-5367> MISC <https://lists.x.org/archives/xorg-announce/2023-october/003430.html> MISC <https://www.debian.org/security/2023/dsa-5534> MISC <https://lists.fedora

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				project.org/archives/list/package-announce@lists.fedoraproject.org/message/sn6kv4xgqjrvaosm5c3cwmvaxo53coip/> MISC <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/sedjn4vfn57k5pooc7bnvd6l6wuucsg6/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xorg-server -- xorg-server	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed.	2023-10-25	not yet calculated	CVE-2023-5380 MISC MISC <https://lists.x.org/archives/xorg-announce/2023-october/003430.html> MISC <https://access.redhat.com/security/cve/cve-2023-5380> MISC <https://www.debian.org/security/2023/dsa-5534> MISC <https://lists.fedora

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				project.org/archives/list/package-announce@lists.fedoraproject.org/message/sn6kv4xgqjrvaosm5c3cwmvaxo53coip/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xorg-server -- xorg-server	A use-after-free flaw was found in xorg-x11-server-Xvfb. This issue occurs in Xvfb with a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode). If the pointer is warped from a screen 1 to a screen 0, a use-after-free issue may be triggered during shutdown or reset of the Xvfb server, allowing for possible escalation of privileges or denial of service.	2023-10-25	not yet calculated	CVE-2023-5574 MISC MISC <https://access.redhat.com/security/cve/cve-2023-5574> MISC <https://lists.x.org/archives/xorg-announce/2023-october/003430.html>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xpand -- it_write-back_manager	Xpand IT Write-back manager v2.3.1 allows attackers to perform a directory traversal via modification of the siteName parameter.	2023-10-26	not yet calculated	CVE-2023-27170 MISC <https://balwurk.com/cve-2023-27170-improper-limitation-of-a-pathname-to-a-restricted-directory/>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. The cleaning of attributes during XHTML rendering, introduced in version 14.6-rc-1, allowed the injection of arbitrary HTML code and thus cross-site scripting via invalid attribute names. This can be exploited, e.g., via the link syntax in any content that supports XWiki syntax like comments in XWiki. When a user moves the mouse over a malicious link, the malicious JavaScript code is executed in the context of the user session. When this user is a privileged user who has programming rights, this allows server-side code execution with programming rights, impacting the confidentiality, integrity and availability of the XWiki instance. While this attribute was correctly recognized as not allowed, the attribute was still printed with a prefix `data-xwiki-translated-attribute-` without further cleaning or validation. This problem has been patched in XWiki 14.10.4 and 15.0 RC1 by	2023-10-25	not yet calculated	CVE-2023-37908 MISC <https://github.com/xwiki/xwiki-rendering/security/advisories/ghsa-6gf5-c898-7rxp> MISC <https://jira.xwiki.org/browse/xrendering-697> MISC <https://github.com/xwiki/xwiki-rendering/commit/f4d5acac451dccaf276e69f0b49b72221e

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	removing characters not allowed in data attributes and then validating the cleaned attribute again. There are no known workarounds apart from upgrading to a version including the fix.			ef5d2f> MISC <https://github.com/xwiki/xwiki-rendering/security/advisories/ghsa-663w-2xp3-5739>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 5.1-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, any user who can edit their own user profile can execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. This has been patched in XWiki 14.10.8 and 15.3-rc-1 by adding proper escaping. As a workaround, the patch can be manually applied to the document `Menu.UIExtensionSheet`; only three lines need to be changed.	2023-10-25	not yet calculated	CVE-2023-37909 MISC <https://github.com/xwiki/xwiki-platform/commit/9e8f080094333dec63a8583229a3799208d773be> MISC <https://jira.xwiki.org/browse/xwiki-20746> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-v2rr-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				xw95-wcjx>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting with the introduction of attachment move support in version 14.0-rc-1 and prior to versions 14.4.8, 14.10.4, and 15.0-rc-1, an attacker with edit access on any document (can be the user profile which is editable by default) can move any attachment of any other document to this attacker-controlled document. This allows the attacker to access and possibly publish any attachment of which the name is known, regardless if the attacker has view or edit rights on the source document of this attachment. Further, the attachment is deleted from the source document. This vulnerability has been patched in XWiki 14.4.8, 14.10.4, and 15.0 RC1. There is no workaround apart from upgrading to a fixed version.	2023-10-25	not yet calculated	CVE-2023-37910 MISC <https://github.com/xwiki/xwiki-platform/commit/d7720219d60d7201c696c3196c9d4a86d0881325> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-rwwx-6572-mp29> MISC <https://jira.xwiki.org/browse/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				xwiki-20334>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 9.4-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, when a document has been deleted and re-created, it is possible for users with view right on the re-created document but not on the deleted document to view the contents of the deleted document. Such a situation might arise when rights were added to the deleted document. This can be exploited through the diff feature and, partially, through the REST API by using versions such as `deleted:1` (where the number counts the deletions in the wiki and is thus guessable). Given sufficient rights, the attacker can also re-create the deleted document, thus extending the scope to any deleted document as long as the attacker has edit right in the location of the deleted document. This vulnerability has been patched in XWiki 14.10.8 and 15.3 RC1 by properly checking rights when deleted revisions of a document are accessed. The only	2023-10-25	not yet calculated	CVE-2023-37911 MISC <https://github.com/xwiki/xwiki-platform/commit/f471f2a392aeeb9e51d59fdfe1d76fccf532523f> MISC <https://jira.xwiki.org/browse/xwiki-20817> MISC <https://extensions.xwiki.org/xwiki/bin/view/extension/index%20application#hpermanentlydeletea

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	workaround is to regularly clean deleted documents to minimize the potential exposure. Extra care should be taken when deleting sensitive documents that are protected individually (and not, e.g., by being placed in a protected space) or deleting a protected space as a whole.			llpages> MISC <https://jira.xwiki.org/browse/xwiki-20685> MISC <https://jira.xwiki.org/browse/xwiki-20684> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-gh64-qxh5-4m33>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. Prior to version 14.10.6 of `org.xwiki.platform:xwiki-core-rendering-macro-footnotes` and `org.xwiki.platform:xwiki-rendering-macro-footnotes` and prior to version 15.1-rc-1 of `org.xwiki.platform:xwiki-rendering-macro-footnotes`, the footnote macro executed its content in a potentially different context than the one in which it was defined. In particular in combination with the include macro, this allows privilege escalation from a simple user account in XWiki to programming rights and thus remote code execution, impacting the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.6 and 15.1-rc-1. There is no workaround apart from upgrading to a fixed version of the footnote macro.	2023-10-25	not yet calculated	CVE-2023-37912 MISC <https://github.com/xwiki/xwiki-rendering/security/advisories/ghsa-35j5-m29r-xfq5> MISC <https://jira.xwiki.org/browse/xrendering-688> MISC <https://github.com/xwiki/xwiki-rendering/commit/5f558b8fac8b716d19999225f

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				38cb8ed0814116e>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 3.5-milestone-1 and prior to versions 14.10.8 and 15.3-rc-1, triggering the office converter with a specially crafted file name allows writing the attachment's content to an attacker-controlled location on the server as long as the Java process has write access to that location. In particular in the combination with attachment moving, a feature introduced in XWiki 14.0, this is easy to reproduce but it also possible to reproduce in versions as old as XWiki 3.5 by uploading the attachment through the REST API which doesn't remove `/` or `\` from the filename. As the mime type of the attachment doesn't matter for the exploitation, this could e.g., be used to replace the `jar`-file of an extension which would allow executing arbitrary Java code and thus impact the confidentiality, integrity and availability of the XWiki installation. This vulnerability has been patched in XWiki 14.10.8 and 15.3RC1. There	2023-10-25	not yet calculated	CVE-2023-37913 MISC <https://jira.xwiki.org/browse/xwiki-20715> MISC <https://github.com/xwiki/xwiki-platform/commit/45d182a4141ff22f3ff289cf71e4669bdc714544> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-vcvr-v426-3m3m>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	are no known workarounds apart from disabling the office converter.			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and	2023-10-25	not yet calculated	CVE-2023-45134 MISC <https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-gr82-8fj2-ggc3> MISC <https://jira.xwiki.org/browse/

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix.			xwiki-20962>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In `org.xwiki.platform:xwiki-platform-web` versions 7.2-milestone-2 until 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, it is possible to pass a title to the page creation action that isn't displayed at first but then executed in the second step. This can be used by an attacker to trick a victim to execute code, allowing script execution if the victim has script right or remote code execution including full access to the XWiki instance if the victim has programming right. For the attack to work, the attacker needs to convince the victim to visit a link like `<xwiki-host>/xwiki/bin/create/NonExistingSpace/WebHome?title=$services.logging.getLogger(%22foo%22).error(%22Script%20executed!%22)` where `<xwiki-host>` is the URL of the Wiki installation and to then click on the "Create" button on that page.	2023-10-25	not yet calculated	CVE-2023-45135 MISC <https://jira.xwiki.org/browse/xwiki-20869> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-ghf6-2f42-mjh9> MISC <https://github.com/xwiki/xwiki-platform/commit/199e27ce7016757e66fa7cea99>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The page looks like a regular XWiki page that the victim would also see when clicking the button to create a page that doesn't exist yet, the malicious code is not displayed anywhere on that page. After clicking the "Create" button, the malicious title would be displayed but at this point, the code has already been executed and the attacker could use this code also to hide the attack, e.g., by redirecting the victim again to the same page with an innocent title. It thus seems plausible that this attack could work if the attacker can place a fake "create page" button on a page which is possible with edit right. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by displaying the title already in the first step such that the victim can notice the attack before continuing. It is possible to manually patch the modified files from the patch in an existing installation. For the JavaScript change, the minified JavaScript			e718044a1b639b>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file would need to be obtained from a build of XWiki and replaced accordingly.			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When document names are validated according to a name strategy (disabled by default), XWiki starting in version 12.0-rc-1 and prior to versions 12.10.12 and 15.5-rc-1 is vulnerable to a reflected cross-site scripting attack in the page creation form. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in XWiki 14.10.12 and 15.5-rc-1 by adding appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix.	2023-10-25	not yet calculated	CVE-2023-45136 MISC <https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e> MISC <https://jira.xwiki.org/browse/xwiki-20854> MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-qcj9-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				gcpg-4w2w>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki -- xwiki	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-2 and prior to version 13.4-rc-1, as well as `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, are vulnerable to cross-site scripting. When trying to create a document that already exists, XWiki displays an error message in the form for creating it. Due to missing escaping, this error message is vulnerable to raw HTML injection and thus XSS. The injected code is the document reference of the existing document so this requires that the attacker first creates a non-empty document whose name contains the attack code. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 13.4-rc-1 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by adding the appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's	2023-10-25	not yet calculated	CVE-2023-45137 MISC <https://github.com/xwiki/xwiki-platform/security/advisories/ghsa-93gh-jgjj-r929> MISC <https://jira.xwiki.org/browse/xwiki-20961> MISC <https://github.com/xwiki/xwiki-platform/commit/ed8ec747967f8a16434806e727a57214a8843581>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WAR and can be patched by manually applying the changes from the fix.			
yxbookcms -- yxbookcms	Cross Site Scripting (XSS) vulnerability in PwnCYN YXBOOKCMS v.1.0.2 allows a remote attacker to execute arbitrary code via the reader management and book input modules.	2023-10-27	not yet calculated	CVE-2023-46503 MISC <https://github.com/pwncyn/yxbookcms/issues/2>
yxbookcms -- yxbookcms	Cross Site Scripting (XSS) vulnerability in PwnCYN YXBOOKCMS v.1.0.2 allows a physically proximate attacker to execute arbitrary code via the library name function in the general settings component.	2023-10-27	not yet calculated	CVE-2023-46504 MISC <https://github.com/pwncyn/yxbookcms/issues/1>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zenario_cms -- zenario_cms	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows a local attacker to execute arbitrary code via a crafted script to the Spare aliases from Alias.	2023-10-25	not yet calculated	CVE-2023-44769 MISC <https://github.com/sromanhu/zenariocms--reflected-xss---alias/tree/main> MISC <https://github.com/sromanhu/cve-2023-44769_zenariocms--reflected-xss---alias/tree/main>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zentao_biz -- zentao_biz	ZenTao Biz version 4.1.3 and before is vulnerable to Cross Site Request Forgery (CSRF).	2023-10-27	not yet calculated	CVE-2023-46375 MISC <https://narrow-payment-2cd.notion.site/zentao-4-1-3-is-vulnerable-to-csrf-cve-2023-46375-2d9d9fc2371f483eb436af20508df915>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zentao_biz -- zentao_biz	Zentao Biz version 8.7 and before is vulnerable to Information Disclosure.	2023-10-27	not yet calculated	CVE-2023-46376 MISC <https://narrow-payment-2cd.notion.site/zentao-8-7-has-information-disclosure-vulnerability-cve-2023-46376-537fae3936b84af583b51b74e6010dd7>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zentao_biz -- zentao_biz	ZenTao Biz version 4.1.3 and before has a Cross Site Scripting (XSS) vulnerability in the Version Library.	2023-10-27	not yet calculated	CVE-2023-46491 MISC <https://foremost-smash-52a.notion.site/zentao-authorized-xss-vulnerability-cve-2023-46491-eea8cbfe2fab4ea78a174e5275309759>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zentao_enterprise_edition -- zentao_enterprise_edition	ZenTao Enterprise Edition version 4.1.3 and before is vulnerable to Cross Site Scripting (XSS).	2023-10-27	not yet calculated	CVE-2023-46374 MISC <https://narrow-payment-2cd.notion.site/zentao-4-1-3-is-vulnerable-to-cross-site-scripting-xss-cve-2023-46374-ebdc61e7a88443b481b649764ba66dee>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyr -- zephyr	Potential buffer overflow vulnerability at the following location in the Zephyr STM32 Crypto driver	2023-10-26	not yet calculated	CVE-2023-5139 MISC <https://github.com/zephyrproject-rtos/zephyr/security/advisories/ghsa-rhrc-pcxp-4453>
zephyr -- zephyr	Potential buffer overflows in the Bluetooth subsystem due to asserts being disabled in /subsys/bluetooth/host/hci_core.c	2023-10-25	not yet calculated	CVE-2023-5753 MISC <https://github.com/zephyrproject-rtos/zephyr/security/advisories/ghsa-hmpr-px56-rvww>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zioncom_holdings_ltd. -- a7000r	An issue in ZIONCOM (Hong Kong) Technology Limited A7000R v.4.1cu.4154 allows an attacker to execute arbitrary code via the cig-bin/cstecgi.cgi to the settings/setPasswordCfg function.	2023-10-27	not yet calculated	CVE-2023-46510 MISC <https://gist.github.com/atonysan/58ace23d539981441bca16ce0f7585e2>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zitadel -- zitadel	ZITADEL is an identity infrastructure management system. ZITADEL users can upload their own avatar image using various image types including SVG. SVG can include scripts, such as javascript, which can be executed during rendering. Due to a missing security header, an attacker could inject code to an SVG to gain access to the victim's account in certain scenarios. A victim would need to directly open the malicious image in the browser, where a single session in ZITADEL needs to be active for this exploit to work. If the possible victim had multiple or no active sessions in ZITADEL, the attack would not succeed. This issue has been patched in version 2.39.2 and 2.38.2.	2023-10-26	not yet calculated	CVE-2023-46238 MISC <https://github.com/zitadel/zitadel/releases/tag/v2.39.2> MISC <https://github.com/zitadel/zitadel/releases/tag/v2.38.2> MISC <https://github.com/zitadel/zitadel/security/advisories/ghsa-954h-jrpm-72pm>

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zpe_systems,_inc. -- nodegrid_os	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/.	2023-10-28	not yet calculated	CVE-2023-43322 CONFIRM <https://psirt.zpesystems.com/portal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023>
palantir -- palantir	The Palantir Tiles1 service was found to be vulnerable to an API wide issue where the service was not performing authentication/authorization on all the endpoints.	2023-10-26	not yet calculated	CVE-2023-30969 MISC

Back to top

Please share your thoughts

We recently updated our anonymous product survey; we’d welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

888-282-0870 central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about> Accessibility </accessibility> Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov> FOIA Requests <https://www.dhs.gov/foia> No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Cybersecurity & AI Scams

BYRON C. CHOU, ESQ.
GASSMAN BAIAMONTE GRUNER, P.C.

A New Generation of **A.I.**

Traditional A.I.

- Identifies patterns in historical data to make predictions
  - Stock market modeling
  - Consumer market trends
  - Weather forecasting

Generative A.I.

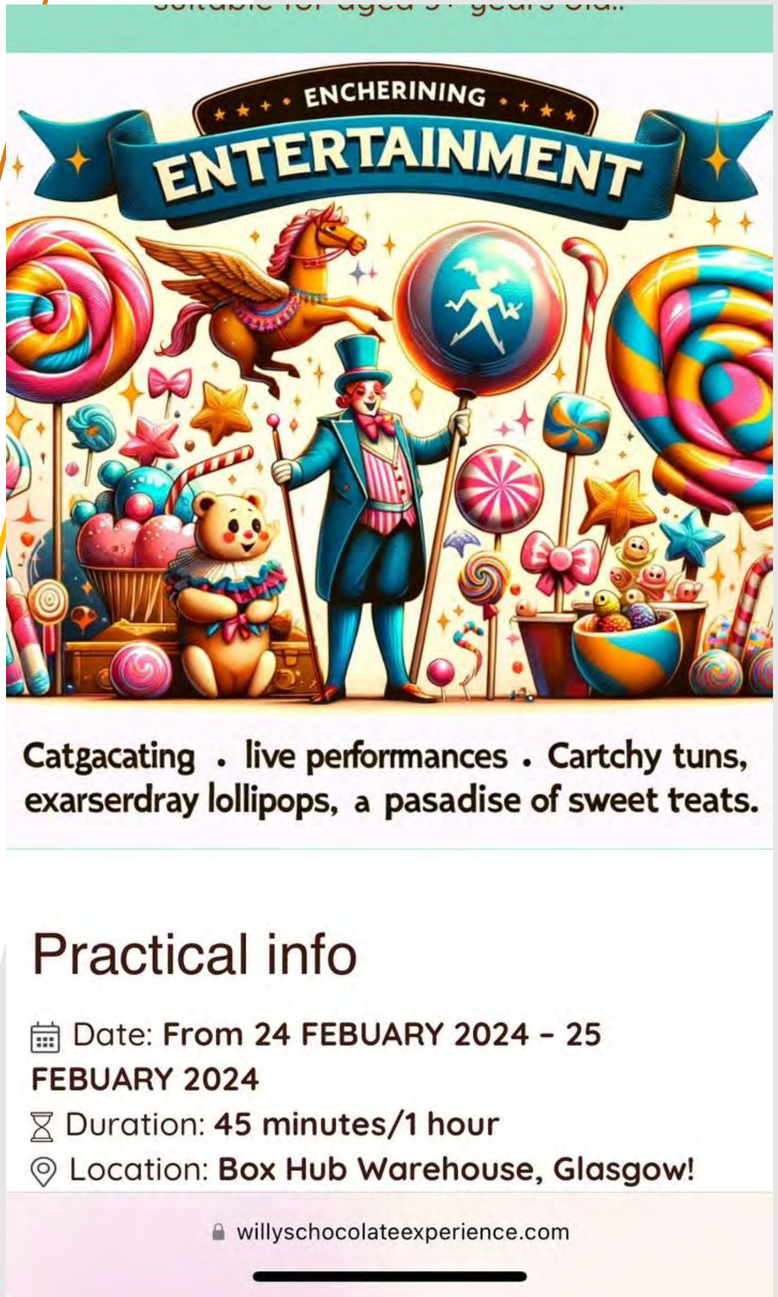
- Uses existing data to “create” new content
  - Recommendation Systems (ex: Netflix)
  - Siri/Alexa/Google
  - Self Driving Cars
  - ChatGPT, Bard, Eleven Labs LLM)

A.I. Advancements =
Advances in A.I.-Based Scams

- Photographic and/or Video Scams
- Voice Scams
  - Boss Voicemail (gift card scam)
  - Family member “emergency”

The Willy Wonka Experience:
A World of Pure Imagination

WILLY'S
CHOCOLATE EXPERIENCE
INDULGE IN A CHOCOLATE FANTASY LIKE NEVER BEFORE -
CAPTURE THE ENCHANTMENT
!



suitable for aged 3+ years old..

Catgacating . live performances . Cartchy tuns, exarserdray lollipops, a pasadise of sweet teats.

Practical info

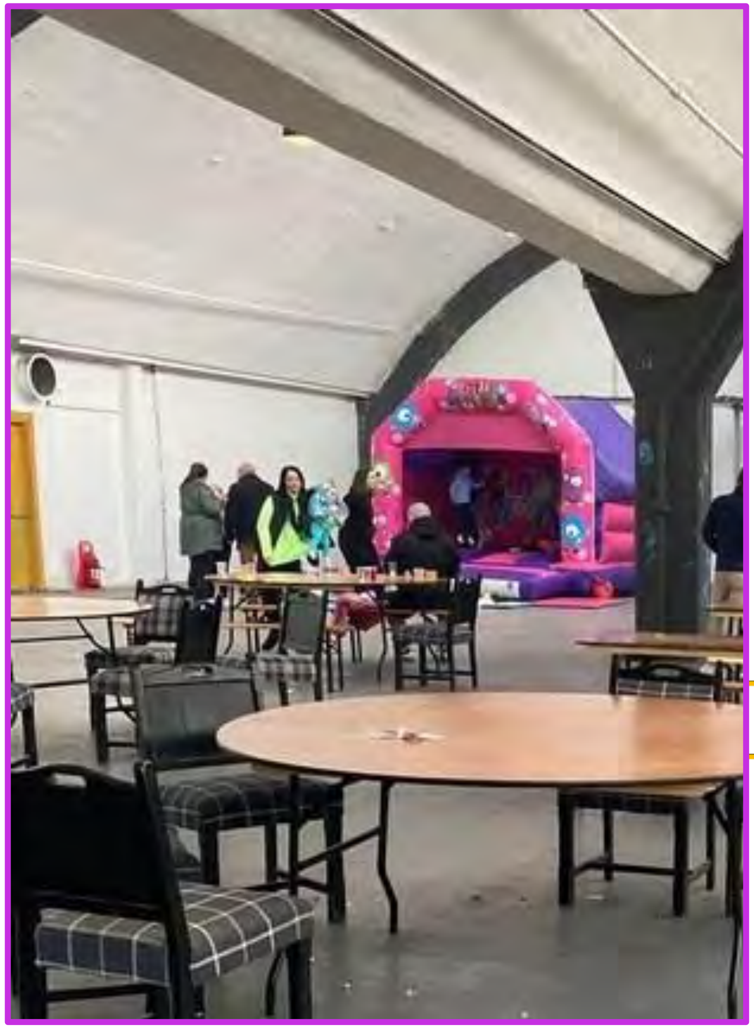
Date: From 24 FEBUARY 2024 – 25 FEBUARY 2024

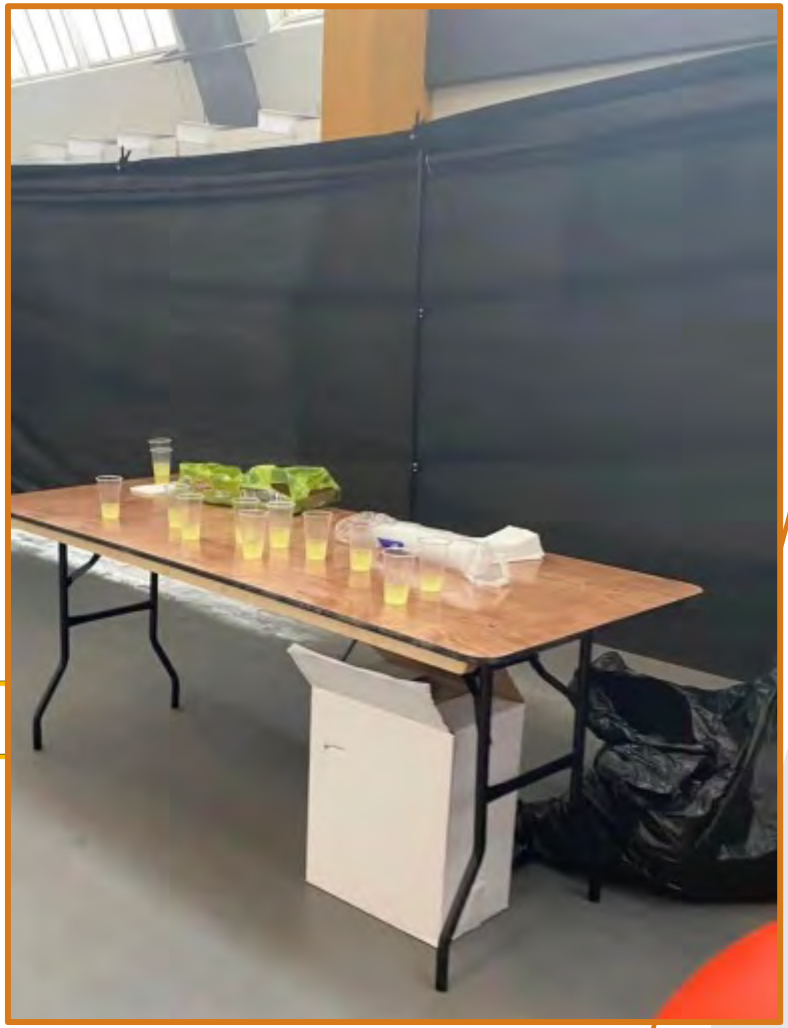
Duration: 45 minutes/1 hour

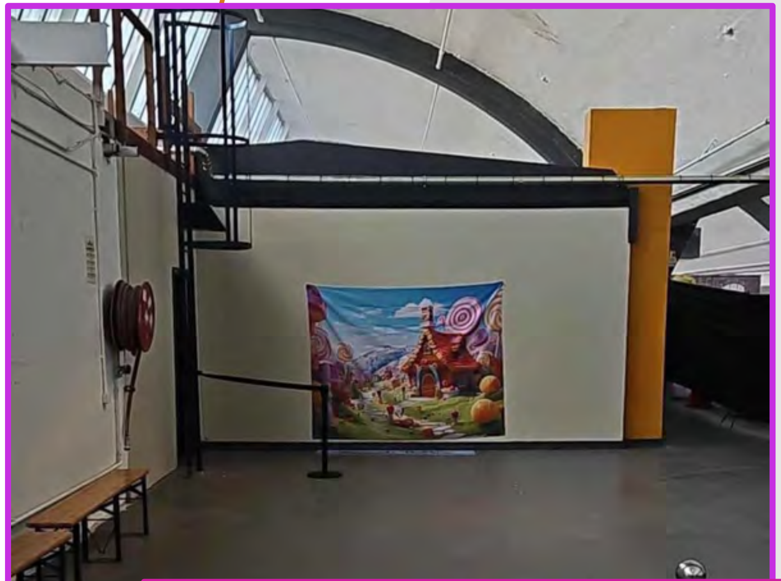
Location: Box Hub Warehouse, Glasgow!

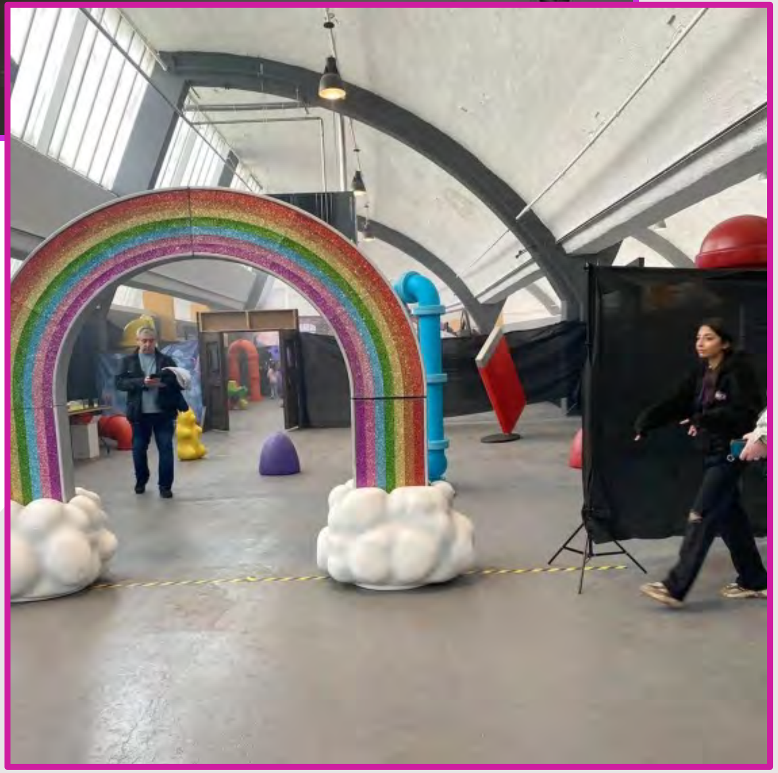
willyschocolateexperience.com

The Willy Wonka Experience: The Not So Magical Reality

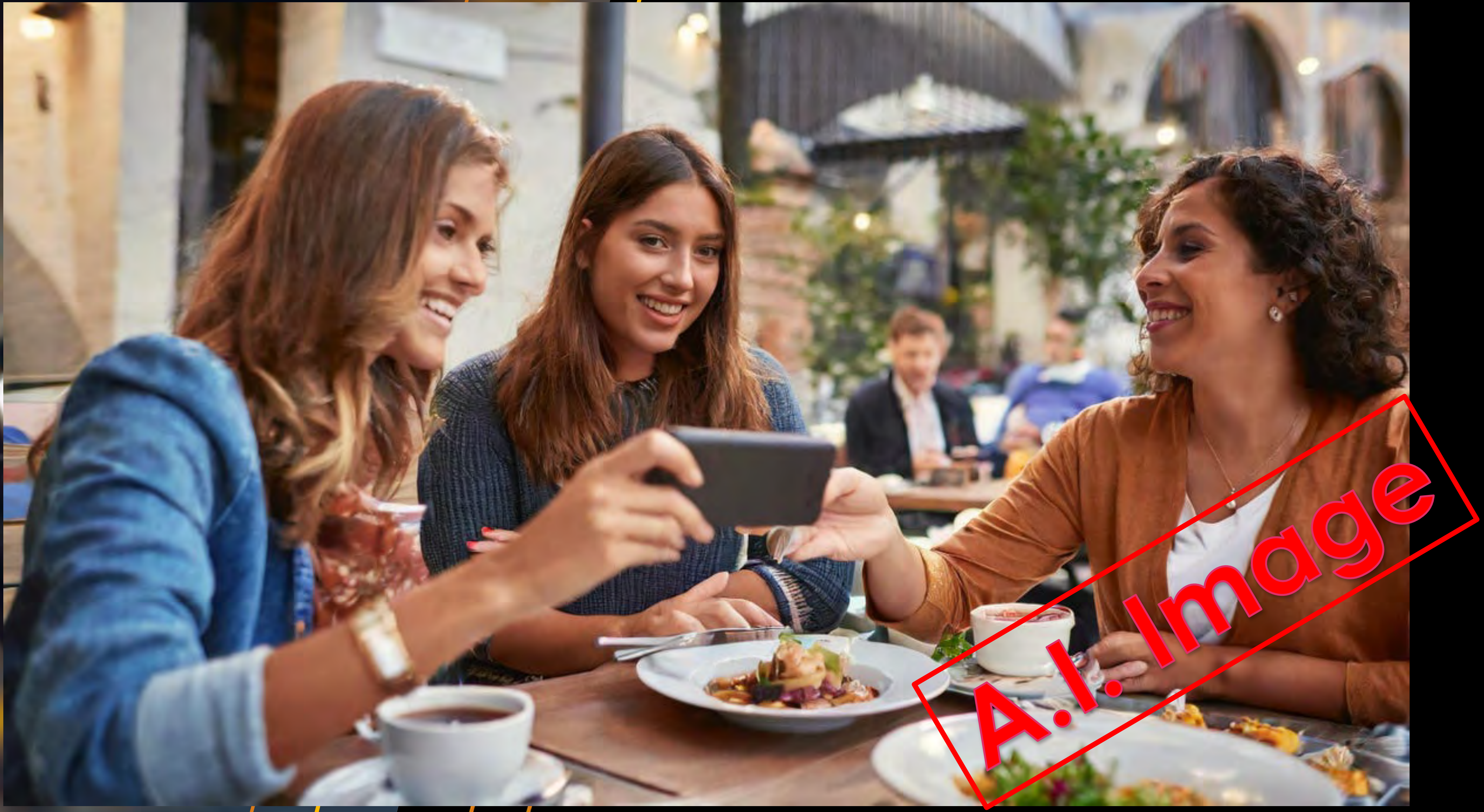




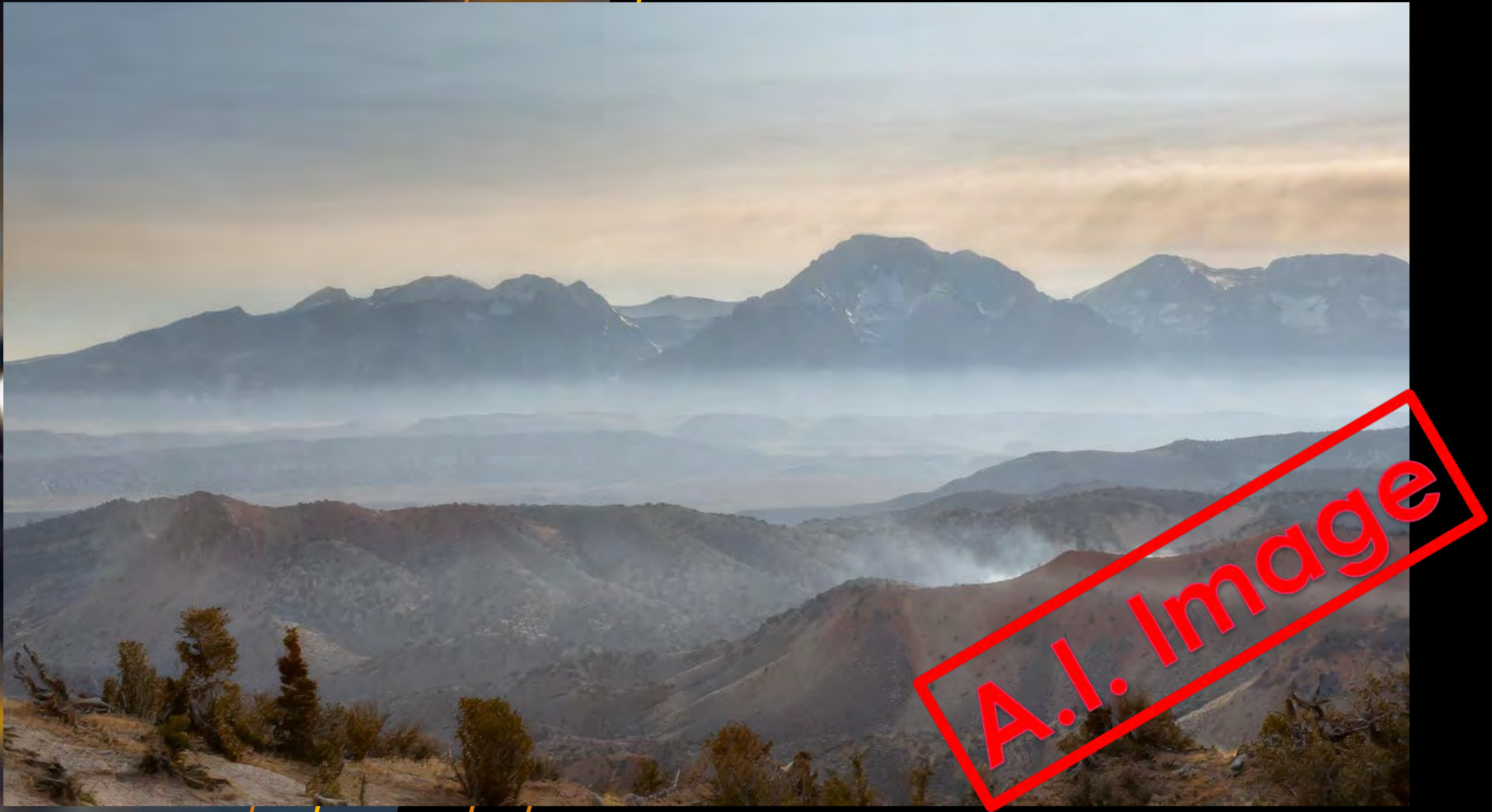




Real or A.I. Generated?

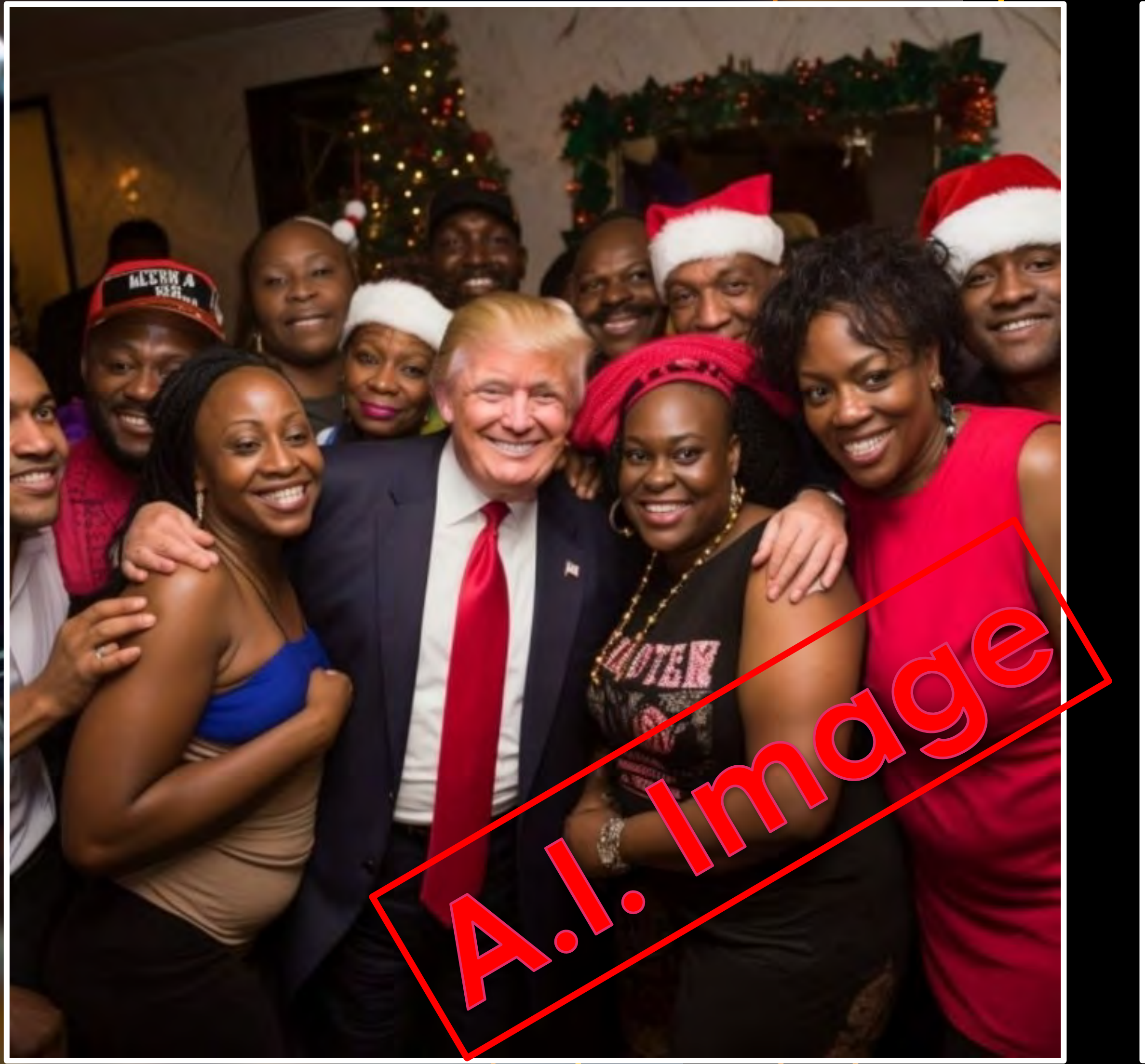


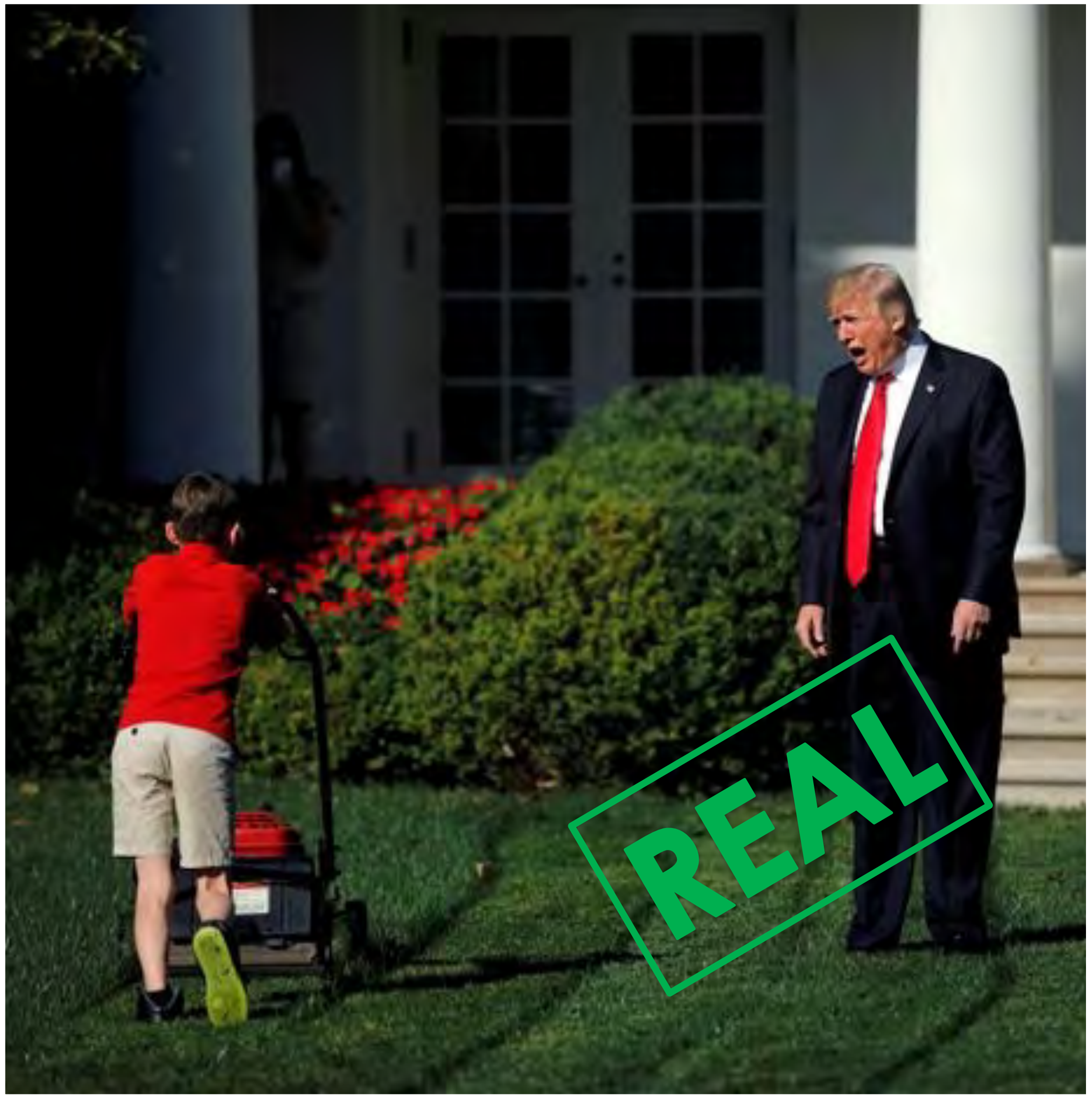
Real or A.I. Generated?



A.I. Image

Real or A.I. Generated?



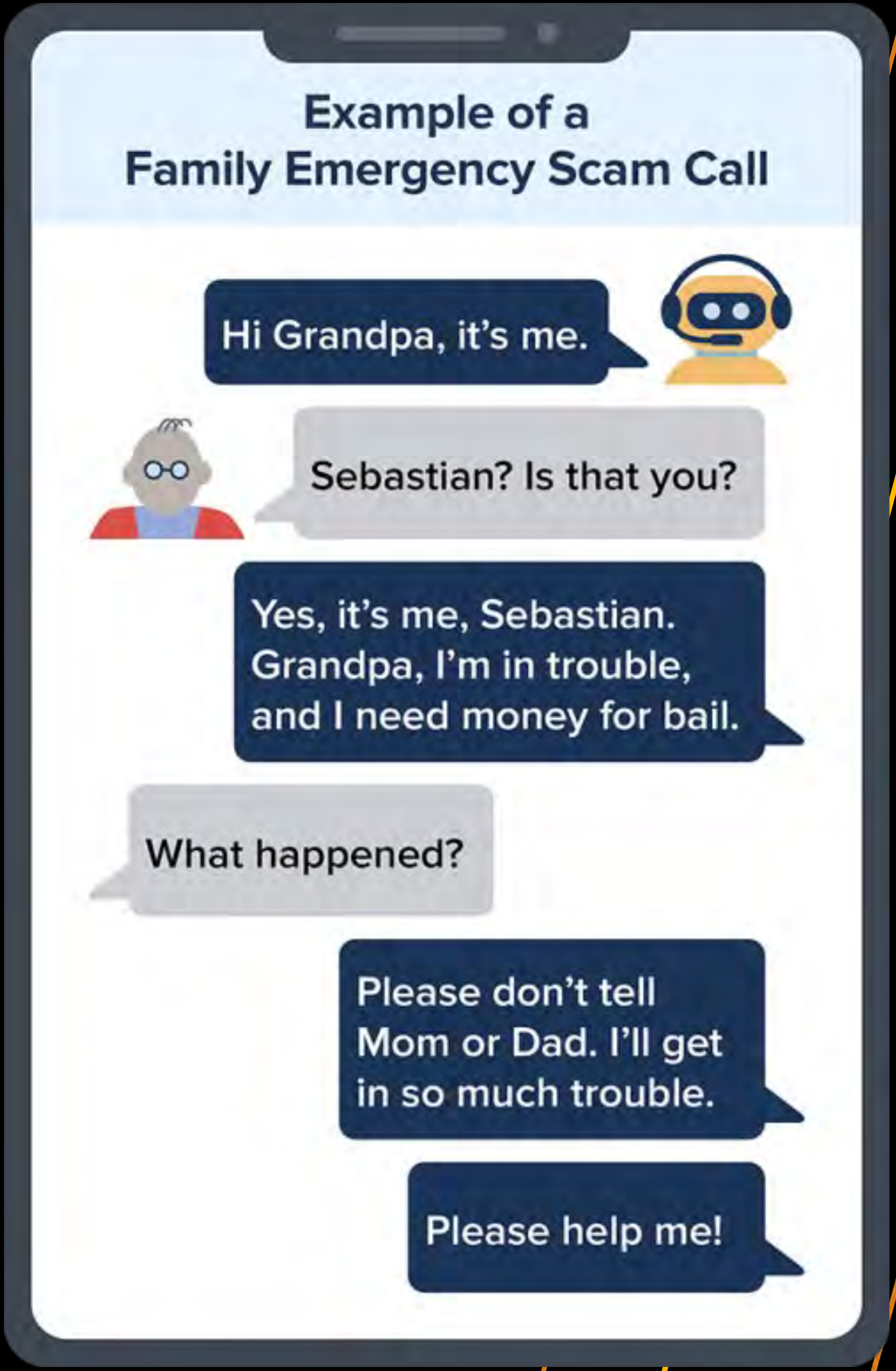


The Growing Problem with Deepfake Videos

Identifying A.I. Generated Videos/Images

- Check for Distortions (e.g., hands, extra limbs, pixelation)
- Warped/unclear facial features, smooth/shiny skin
- Poor image quality (blurry, odd shadows, light flickering, unnatural blinking)
- Unnatural body language
- Nonsensical background text
- Reverse Image Search

- ChatGPT Image Generator Demonstration



Example of a Family Emergency Scam Call

Hi Grandpa, it's me.

Sebastian? Is that you?

Yes, it's me, Sebastian. Grandpa, I'm in trouble, and I need money for bail.

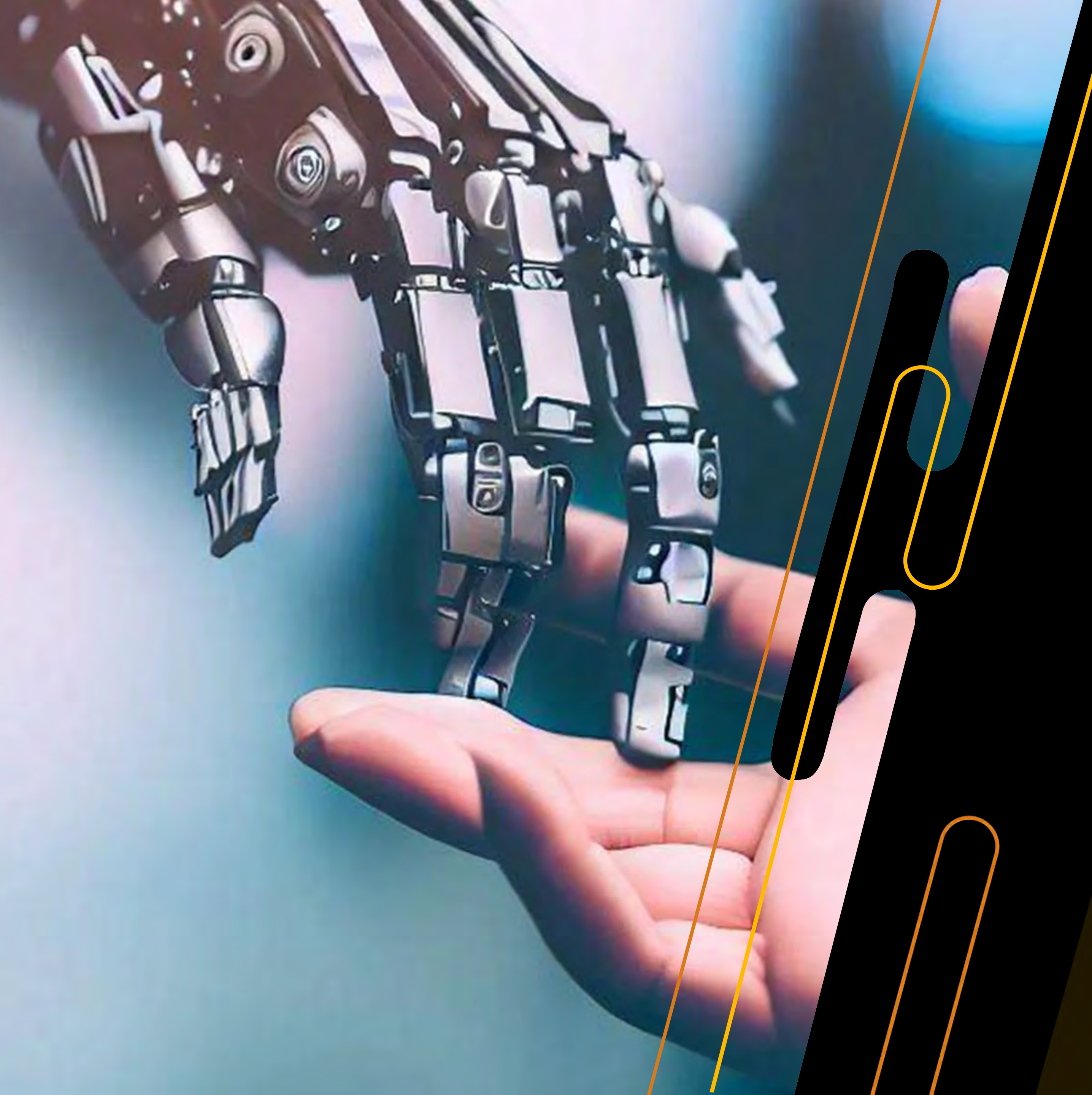
What happened?

Please don't tell Mom or Dad. I'll get in so much trouble.

Please help me!

Protect Against A.I. Scams

- Is this a real family member or cloned voice?
- Don't trust the voice and VERIFY THE STORY
- Resist the urge to act immediately
- Train your staff/office
- Never send money online
- Be careful what you post online (info, photos, videos, etc.)
- Have a "Family Safe Word"



Questions?

Malwarebytes LABS

Search Labs

SUBSCRIBE

NEWS | PERSONAL

AI used to fake voices of loved ones in “I’ve been in an accident” scam

Posted: January 17, 2024 by Pieter Arntz

The San Francisco Chronicle tells a story about a family that almost got scammed when they heard their son’s voice telling them he’d been in a car accident and hurt a pregnant woman.

quickly.

Sometimes it's a pregnant woman who is hurt, sometimes it's a diplomat.

In earlier days of scams like these, success depended a great deal on the criminal's skills at social engineering, but rapid advancements in Artificial Intelligence (AI) mean scammers can now easily and convincingly fake the "voice" of the relative that is the supposed victim of the accident.

What better way to make the victim believe that something bad has happened than hearing their loved one cry out for help in their own voice. With the help of various AI powered tools, criminals can easily compose fragments based on a short voice clip they found online.

FBI Special Agent Robert Tripp said:

> "Now criminals can fabricate a voice using AI tools that are available either in the public domain for free, or at a very low cost."

The criminals will keep that part of the communication short, so the target is unable to ask the relative any questions about what happened. While it is possible to fake entire conversations with the help of AI, the tools that can do that are much harder to operate. The criminal would have to type out the responses very quickly and the target might get suspicious. In the story from the San Francisco Chronicle, the phone was "taken over" by the so-called police officer at the scene of the accident, who told the parents that their son would be taken into custody.

This was later followed a cold call by someone posing as legal representative for their son, asking for money to for bail. The intended victims got suspicious when the so-called lawyer said he'd send a courier to pick up the bail money.

The FBI says it has received more than 195 complaints about this type of scam that it refers to as "grandparent scams." It reports nearly $1.9 million in losses, from January through September of 2023.

How to avoid scams like this

One of the main tools for the imposters is the amount of information they can round up about the target. Their main sources will include social media and phishing.

- Do not answer telephone calls from numbers you do not recognize or calls from private numbers.
- Ask for the caller’s telephone number and check it.
- If necessary, try to reach your allegedly implicated family member by phone. If you can’t reach them directly, call someone else who might know where they are.
- Hang up if in doubt and never give financial or personal information to the caller.
- If you receive or have received such a call, please notify the police immediately and under no circumstances respond to the perpetrators’ demands.

SHARE THIS ARTICLE

https://www.wsj.com/tech/cybersecurity/microsoft-still-facing-intrusions-from-russian-sponsored-hacking-group-33208acd

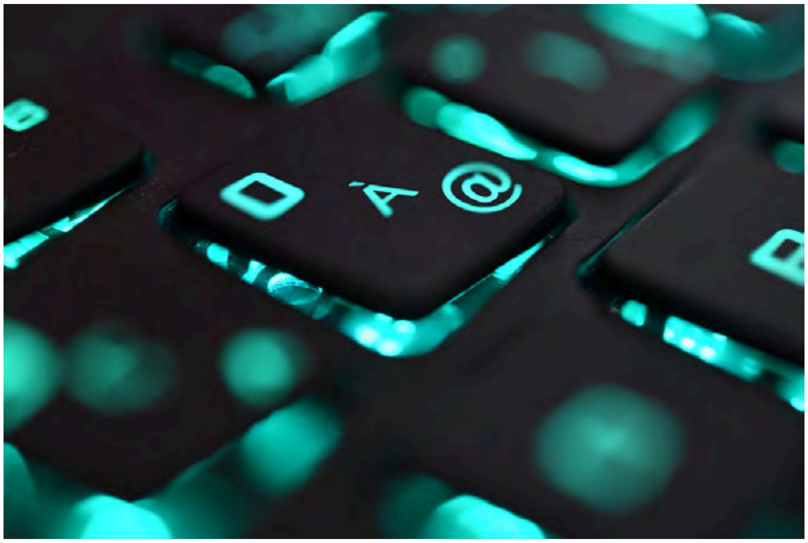
TECHNOLOGY | CYBERSECURITY

Microsoft Says Russian-Sponsored Hackers Still Using Stolen Information

Company said in January that hackers took information from email accounts of its leadership team and other employees

By Dean Seal Follow

March 8, 2024 9:57 am ET



Microsoft said the attack doesn't appear to have compromised customer-facing systems. PHOTO: FRED TANNEAU/AGENCE FRANCE-PRESSE/GETTY IMAGES

Microsoft MSFT **-0.42%** ▼ said a Russian state-sponsored hacking group that stole information from its senior leadership team is still using that information to gain unauthorized access to its internal systems.

The technology company disclosed in January that the group, which it has identified as Midnight Blizzard, had extracted information from a small percentage of employee email accounts, including members of its senior leadership team and employees in its cybersecurity and legal teams.

Since that disclosure, the group has used that information to gain access to Microsoft's source code repositories and internal systems, the company said Friday.

The volume of some aspects of the attack, including password sprays, jumped 10-fold in February compared with the already large volume Microsoft encountered in January, it said.

"Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus," Microsoft said.

The company said that its investigations of Midnight Blizzard activities are continuing and that it is coordinating efforts with federal law enforcement.

The attack doesn't appear to have compromised customer-facing systems and hasn't had a material impact on operations, Microsoft said. It hasn't determined whether the incident will likely impact its financial condition.

In a blog post last August, Microsoft said it had detected Midnight Blizzard, previously known as Nobelium, launching targeted social-engineering attacks that used Microsoft Teams chats to phish for credentials.

The former Nobelium group has been linked by U.S. authorities to the Foreign Intelligence Service of the Russian Federation and is known for its involvement in the massive SolarWinds hack of 2020.

Write to Dean Seal at dean.seal@wsj.com

Appeared in the March 9, 2024, print edition as 'Russian Hackers Continue to Test Microsoft'.

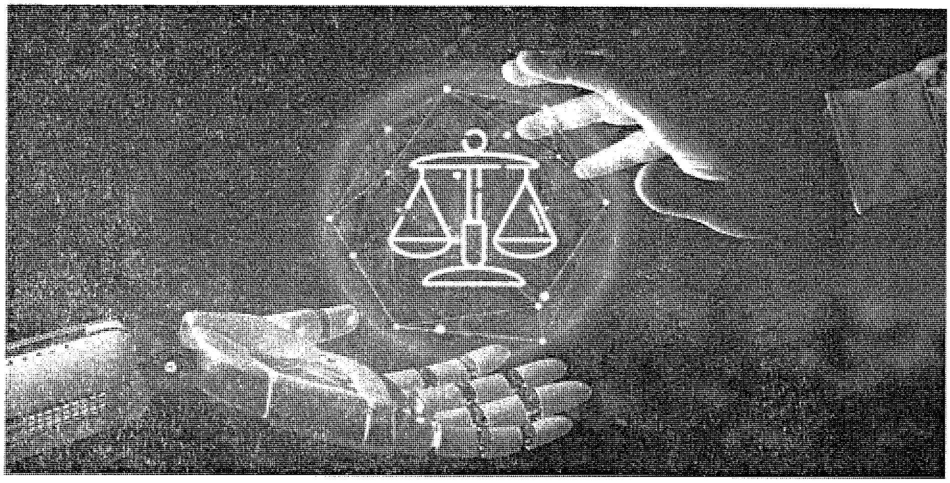
ETHICS

Lawyers should take these precautions when using artificial intelligence, Florida ethics opinion says

BY DEBRA CASSENS WEISS (HTTPS://WWW.ABAJOURNAL.COM/AUTHORS/4/)

JANUARY 23, 2024, 12:28 PM CST

Like 24 Share Post Share



Generative artificial intelligence—which can generate new content based on a prompt—has the potential to "dramatically improve the efficiency of a lawyer's practice," but it also can pose ethical concerns. (Image from Shutterstock)

Generative artificial intelligence—which can generate new content based on a prompt—has the potential to "dramatically improve the efficiency of a lawyer's practice," but it also can pose ethical concerns, according to a Florida Bar ethics opinion (https://www.floridabar.org/etopinions/opinion-24-1) approved Jan. 19.

One of the pitfalls is that generative AI can "hallucinate" or create "inaccurate answers that sound convincing," the opinion says, citing an October 2023 article (https://www.abajournal.com/web/article/vlex-releases-new-generative-ai-legal-assistant) from ABAJournal.com.

Because of the concerns, lawyers using generative AI should develop policies for reasonable oversight of the technology, the opinion says.

"Lawyers are ultimately responsible for the work product that they create regardless of whether that work product was originally drafted or researched by a nonlawyer or generative AI," the opinion says.

The opinion also warns that lawyers may not delegate any act that could constitute the practice of law to generative AI. Acts that can't be delegated would include the negotiation of claims or other functions that require a lawyer's personal judgment and participation.

Nonlawyers are allowed to conduct initial interviews with a prospective client, but using an "overly welcoming" generative AI chatbot for this function could pose problems, the opinion says. The chatbot could wrongly offer legal advice, fail to identify itself as a chatbot at the outset, and fail to include disclaimers limiting formation of an attorney-client relationship.

The opinion also says that lawyers should:

- Preserve the confidentiality of client information. Self-learning AI programs continue to develop responses with new input. The danger is that a client's information revealed in a lawyer query could be stored in the AI program and revealed in response to future inquiries by third parties.

"It is recommended that a lawyer obtain the affected client's informed consent prior to utilizing a third-party generative AI program if the utilization would involve the disclosure of any confidential information," the opinion says.

In-house generative AI programs may mitigate confidentiality concerns. If a third party does not host or store AI data, a lawyer is not required to obtain the client's informed consent, the opinion concludes.

- Ensure that fees and costs are reasonable. Generative AI programs may make a lawyer's work more efficient, but lawyers should not use the efficiency to falsely inflate claims of billable time.

"Lawyers may want to consider adopting contingent fee arrangements or flat billing rates for specific services, so that the benefits of increased efficiency accrue to the lawyer and client alike," the opinion says.

- Comply with applicable ethics and advertising regulations. Lawyers can't advertise that their generative AI is better than technology used by other lawyers unless the claim is verifiable. Lawyers who use AI chatbots for advertising and intake will be responsible if the chatbot provides misleading information to prospective clients or if its communications are "inappropriately intrusive or coercive," the opinion says.

The opinion warns that AI is still in its infancy, and the ethical concerns addressed should not be treated as exhaustive.

Florida Bar News (https://www.floridabar.org/the-florida-bar-news/board-of-governors-adopts-ethics-guidelines-for-generative-ai-use), Reuters (https://www.reuters.com/legal/transactional/lawyers-use-ai-spurs-ethics-rule-changes-2024-01-22) and Bloomberg Law (https://news.bloomberglaw.com/litigation/ai-guidance-from-florida-bar-builds-on-familiar-ethics-rules) covered the ethics opinion.

Reuters noted that California has issued AI guidance (https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf) that is also based on ethics obligations. And bar associations in at least six other states are also considering recommendations for lawyers' responsible use of AI, the article says.

Bloomberg Law spoke with Brian David Burgoon, chair of the ethics committee that developed the opinion.

"It's a game-changer in the practice of law," Burgoon told Bloomberg Law.

AI can provide a competitive edge to lawyers who use it responsibly, but ethical guidance is needed.

“There’s good tools out there, but there are some bad problems that can come with them,” he told the publication.

Give us feedback, share a story tip or update, or report an error.

AI Can Tackle New Tasks at Companies. But It's Costly.

Many executives are still figuring out how, and how fast, to go with generative AI

BY CHIP CUTTER

CISCO Systems recently had a problem: A manager and a new employee at the technology giant struggled to work together. Both people felt frustrated. What to do?

As is increasingly the answer inside large U.S. companies, leaders turned to generative AI for help. Cisco's human-resources team uploaded chat logs between the employee and manager, hoping to suss out the source of the tension. (Both people consented to this, Cisco says.)

After quickly sifting through pages of discussions, the software came up with an answer: The manager didn't feel heard as the employee asked some of the same questions over and over. The employee, seeking as much clarity as possible, could sense a high degree of frustration. The company says knowing the details helped the relationship improve.

"There was just this 'Aha!' " says Francine Katsoudas, Cisco's top human-resources executive.

Companies are using generative AI for ever more sophisticated tasks—including work such as deciphering friction between colleagues at Cisco, once exclusively the domain of well-paid knowledge workers. This change is fueling predictions of workplace transformation—both ominous and optimistic.

Some fear a wave of disrup-

Please turn to page R2

WSJ 3/11/24

Companies Experiment With What Jobs AI Can Best Handle

Continued from page R1

tive job losses, as AI becomes better able to take over the work long done by knowledge workers. The thinking goes: Do you really need so many people in the HR department if the software can do it cheaper and more quickly?

Others say such concerns are overblown. They anticipate that AI will unlock innovations and usher in a higher quality of life.

JPMorgan Chase CEO Jamie Dimon has said that AI might require future generations to work only 3½ days a week. Technology will invent cures for cancer, Dimon said last year, and allow more people to live to 100 by finding breakthroughs impossible to achieve through the mind alone.

Others say AI will free people to do more of what interests them. Within 10 years, AI will take on "80% of 80% of the jobs that exist today," said Vinod Khosla, founder of venture-capital firm Khosla Ventures, in a Wall Street Journal interview last fall. "The need to work in society will disappear within 25 years for those countries that adapt these technologies."

Among executives on the ground, however, the situation is more murky. Many say they are now trying to separate hype from reality to come up with their own answer to a fundamental question: How pervasive will AI become in corporate life, and how quickly should I adopt it in my own company?

"At the end of the day, it's the human interaction with the technology that's going to make or break the impact," says Marc Casper, CEO of life-sciences company **Thermo Fisher Scientific**, which is using generative AI in corporate functions such as marketing to help write advertising content.

A host of hurdles

Some roles will significantly change. Research by the McKinsey Global Institute has found that, with generative AI and other tools, 30% of the hours worked today could be automated by 2030.

Even so, the hurdles to broad AI adoption are many. Regulations remain in flux. Adopting AI means added costs. Companies selling AI tools, including OpenAI, face legal challenges, including from prominent executives like Elon Musk. Some executives also fear putting proprietary information inside large language models.

Labor unions have pushed back against AI; in Hollywood, the use of AI was a central issue in strikes last year among unions representing actors and writers.

Getting people to change how they do their jobs and to adopt AI tools also takes time.

"It's one thing for the CEO and the board and the management team to understand AI. But to really succeed you have to bring everybody along, and so that's actually the hardest part," says Clara Shih, who oversees artificial intelligence at **Salesforce**.

No job-killer, yet

In interviews with more than two dozen executives in recent weeks, many executives say they haven't seen evidence yet that artificial intelligence is the job-killer—at least in the next few years—that some initially suspected when OpenAI's ChatGPT emerged more than a year ago. This is partly because many companies are still working to understand all that AI can do beyond work in call centers and among software coders.

ROB DOBI

A variety of experiments are under way. Some companies are now rolling out AI tools to create photos for marketing projects or to analyze contracts. Others hope it can be used to produce training videos more quickly. Bob Toohey, chief human resources officer at the insurer **Allstate**, recently experimented with an AI tool that could allow the company to create internal videos in his voice or others from text prompts to allow for faster on-the-job learning.

At **Ecolab**, a water-management and infection-prevention company, executives are testing generative AI to analyze earnings reports from rivals and to help in preparing for its own investor calls.

Christophe Beck, Ecolab's chief executive officer, says the company's finance team is using generative AI to parse earnings-call transcripts from competitors, asking questions such as: "What were the highlights that the CEO shared?" and "Where was the CEO the most secure? Where was the CEO least secure?"

With some AI software priced at $30 per employee a month, a number of executives have questioned the price tag. Man yemployers are finding that they are spending more money on AI than they are realizing in productivity improvements, says Christoph Schweizer, CEO of Boston Consulting Group. He encourages companies not to take a wait-and-see approach, saying they should try AI tools now to gain an edge.

Some companies say they won't fire existing employees, but they may not need to hire as significantly in the future.

A survey from consulting giant **Accenture** in January found that roughly 60% of workers fear AI could eliminate their jobs. Manish Sharma, CEO of North America for Accenture, says that, based on his interactions with clients, he is convinced that AI will create more roles than it replaces. The jobs, though, might be different.

At the San Francisco company Tome, a generative AI storytelling and presentation platform, CEO Keith Peiris says he has begun looking to hire what he calls "resourceful generalists," versus specialists with the exact experience he may need, knowing smart professionals can use AI software to amplify their knowledge and solve new problems that emerge.

Chip maker **Qualcomm** is looking to create more marketing content for social media like TikTok. Instead of hiring an army of additional video editors, Don McGuire, the company's chief marketing officer, has decided to build a generative-AI creative studio in Mexico City. It plans to hire up to a dozen people there. "It will be built with people, but with tools that are rooted in Gen AI," McGuire says.

Chip Cutter is a reporter covering workplace issues in The Wall Street Journal's New York bureau. Email him at ***chip.cutter@wsj.com.***

WSJ 3/9-10/24

Russian Hackers Continue to Test Microsoft

By Dean Seal

Microsoft said a Russian state-sponsored hacking group that stole information from its senior leadership team is still using that information to gain unauthorized access to its internal systems.

The technology company disclosed in January that the group, which it has identified as Midnight Blizzard, had extracted information from a small percentage of employee email accounts, including members of its senior leadership team and employees in its cybersecurity and legal teams.

Since that disclosure, the group has used that information to gain access to Microsoft's source code repositories and internal systems, the company said Friday.

The volume of some aspects of the attack, including password sprays, jumped 10-fold in February compared with the already large volume Microsoft encountered in January, it said.

"Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus," Microsoft said.

The company said that its investigations of Midnight Blizzard activities are continuing and that it is coordinating efforts with federal law enforcement. The attack doesn't appear to have compromised customer-facing systems and hasn't had a material impact on operations, Microsoft said. It hasn't determined whether the incident will likely impact its financial condition.

In a blog post last August, Microsoft said it had detected Midnight Blizzard, previously known as Nobelium, launching targeted social-engineering attacks that used Microsoft Teams chats to phish for credentials.

The former Nobelium group has been linked by U.S. authorities to the Foreign Intelligence Service of the Russian Federation and is known for its involvement in the massive SolarWinds hack of 2020.

KEYWORDS | CHRISTOPHER MIMS

A Guide to the Many Flavors of AI Today

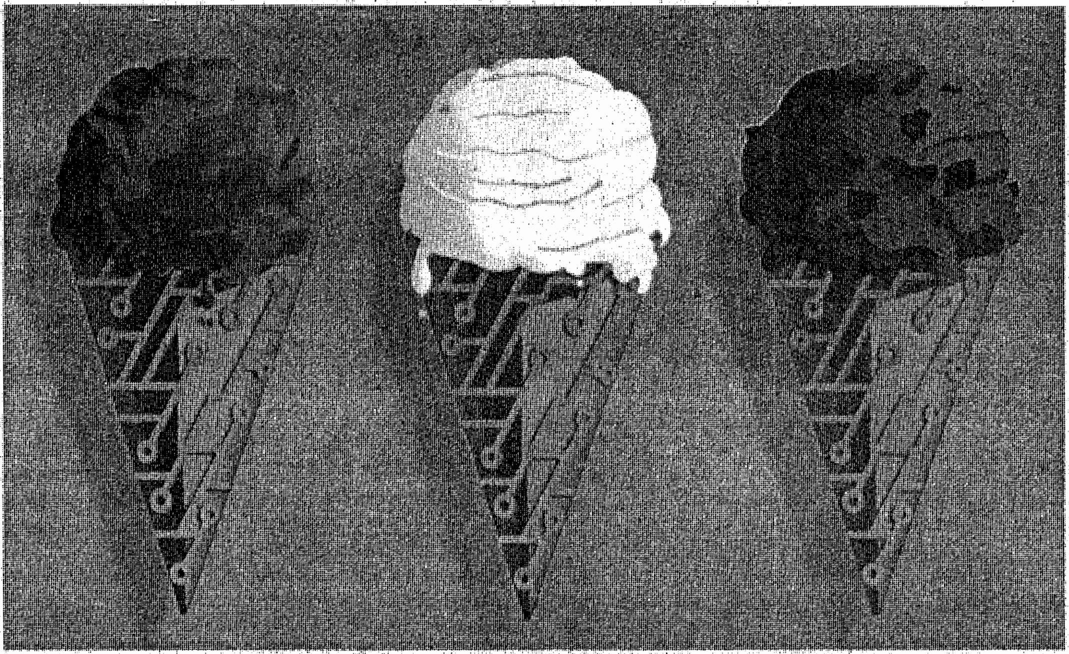
Open AI, Google, Meta or Anthropic? Different versions work best for different business needs

We're all being deluged with news about how the latest generation of AI is transforming people's lives, helping businesses be more productive, and even leading to layoffs. But that flood of information doesn't help anyone answer the most basic question about these AIs: Which is best?

So I canvassed executives, engineers and researchers who are knee-deep in the process of applying the world's most powerful AIs to real world problems, to find out what they have learned.

Their answers surprised me. There was plenty of practical advice about the relative strengths and weaknesses of AIs from Google, OpenAI, Anthropic and Meta. But the overall message was that the best AI for any task depends on both the user and the task. Their insights also offer a glimpse of where the entire field of AI is going.

Companies can now either embrace the potential cost savings and productivity boost of generative AI—which some researchers believe is on the path to a "general" or humanlike AI—or risk losing out to competitors who will.



JARRED BRIGGS

Your AIs Are Employees

Today's most powerful AIs are only accessible through the cloud. This makes it easy to test them by feeding them documents, images and text, but also means that businesses have limited ability to alter their behavior.

Testing these AIs is more like hiring an employee than just buying a piece of software off the shelf, says Mark Daley, chief AI officer of Western University in Ontario.

"People expect the chatbot to work right out of the box, but you have to spend time trying them and see which of these will deliver, just like you do with an employee," he adds.

Daley has found that all of the major large language models—including those from OpenAI, Anthropic, Google and Cohere, a startup that only offers its models to businesses—have their strengths and weaknesses. Which one to use depends on a person's preferences and the task at hand, and it pays to experiment with them.

Buying ChatGPT

Other companies appear to be catching up with the capabilities of OpenAI, but OpenAI's models remain, for now, the standard by which all others are judged. Earlier this week, Anthropic rolled out Claude 3, a new large language model which the company claims beats the gold standard GPT-4 on every benchmark.

"We are using OpenAI like crazy," says Brad Schneider, chief executive of Nomad Data, a company that helps large companies use AI. Nomad Data uses OpenAI to digest, summarize and search within huge libraries of documents, such as legal briefs, court cases and insurance claims.

After trying all of the most-capable large-language models, Schneider's company found that none are as good as OpenAI for these kinds of document-processing tasks. Previous versions of Anthropic's Claude and current versions of Google's Gemini both hallucinated too often, he found.

Google senior vice president Prabhakar Raghavan recently wrote that hallucination is a challenge common to all large language models, but that "this is something that we're constantly working on improving." Anthropic President Daniela Amodei has said that it is "very, very hard" to get the hallucination rate in such models to zero. The company has said that its latest model is twice as likely as its previous one to answer questions accurately.

What Counts for AI

In addition to accuracy, the other two big considerations are speed and cost, says Eric Olson, chief executive of Consensus, a scientific search engine.

On a search engine, users expect a response within seconds. Because Consensus pairs its search results with summaries of scientific papers made by GPT-4, the company needs those summaries to be generated nearly instantaneously.

For Olson's purposes, this means the only truly suitable model is OpenAI's GPT-4 "turbo," which can get a user a response within 1.5 seconds, versus twice as long with regular GPT-4. Google's Gemini and Anthropic's Claude are also slower than OpenAI's models, he adds.

That said, this kind of performance comes at a cost. OpenAI and its competitors charge business users of their systems by the token—in essence, by the word—to process their requests.

"We have cases where one question someone asks can cost $50," says Schneider. That could happen if, for example, someone asks a specific question about a collection of 5,000 legal documents, because the number of calls to OpenAI's systems could be in the tens of thousands.

True Today, Tomorrow?

Generative AI is a technology evolving at a rate not seen since the go-go days of the early internet itself. Anthropic's release of a model that seems every bit as capable as OpenAI's, despite having a smaller team and having been founded much more recently, suggests that large language models may become commodities. At that point, the only thing that will matter will be which company can offer the fastest response at the lowest price.

The beneficiary of that fierce competition will be companies large and small, which could see significant increases in the productivity of their employees. Those gains will come at a fraction of the cost of paying humans to do the same knowledge work. The implications for the future of white collar jobs are obvious—and worrisome.

AI Is Coming! Tips for Keeping Calm and Carrying On

Will the advances of AI bring doom or bliss? Maybe a bit of both?

SJ
19-10/24

BY HENRY ALFORD

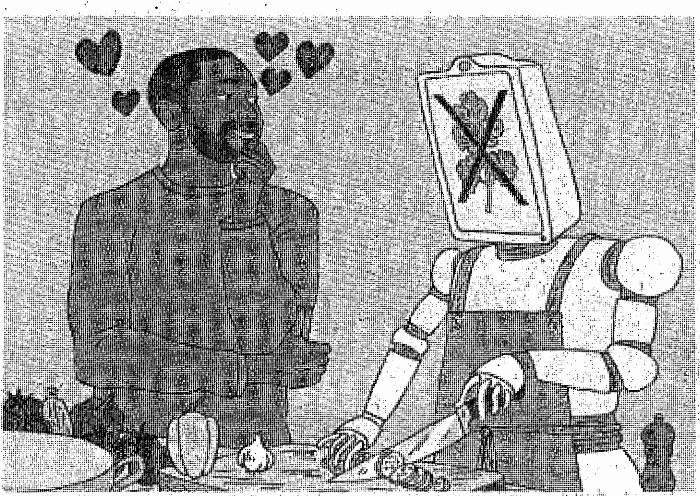
SURE, AI is taking over the world, but that's not all bad! Here are some suggestions for braving the coming revolution.

Relish the thought that, shorn of the need to work, you'll be able to devote yourself to more pressing issues, like why country singers are always telling us where they come from.

Consider that carbon dioxide sequestration can succeed only with AI-powered risk modeling. Don't worry that this sentence is incomprehensible to non-Nobel Prize winners.

Take comfort in the fact that the drivers of self-driving cars are not talking on their phones while driving because they *are* phones.

Ease your anxieties about the earning potential of your artist friends because most AI-generated art looks like it was born on the side of a van.


PETER ARKLE

Entertain the idea that AI robots might fall somewhere between amoral predators bent on destroying humanity and bowtie-wearing manservants with chirpy English accents.

Savor the prospect of seeing the very humans who are the least subject to morality and ethics—politicians—regulating AI's morality and ethics.

Contemplate the potential enchantments of a companion bot: At last, a partner who remembers that you are allergic to cilantro and Meg Ryan.

Remember that some Victorians thought that the novel was the death of literature.

Savor the fact that the snotty chess master in your daughter's sixth-grade class is about to get trounced.

Avoid obsessing over whether or not you sounded passively aggressive toward a robot.

Imagine being able to decisively end all conversations simply by glancing skyward and delivering a withering "But is it scalable?"

Relish the thought of buying your outsized, bearlike friend a T-shirt emblazoned "BIG DATA."

Compare the current anxiety about teeming, unregulated AI with our previous anxiety about teeming, unregulated drones: 15 years ago everyone worried that drones would soon be swarming like Hitchcock's birds, but mostly they have delivered hours and hours of videos of waterfalls.

Look forward to the advent of an a cappella bot group, the Algorhythms.

Imagine becoming so informed about AI that you have a conversation about epistemological uncertainty in which you deploy the terms "Bayesian" and "probabilistic" with the cool of Catherine Deneuve blowing a smoke ring.

Consider the possibility that, once everyone's troubles with the law are recorded in a way that is instantly accessible to strangers, scofflaws will be less likely to commit even tiny crimes, such as clipping their toenails in public.

Make peace with the idea that your grandchildren may spend their lives as slaves in the lithium mines.

Spend pleasant hours imagining that a machine, which can withstand hostile environments far better than humans, can go to your cousin's wedding for you.

Look forward to your very own chatbot assistant who, unlike Siri or Alexa, doesn't sound like she's composed of equal parts gaseous vapor and pause button.

Appreciate how fewer tedious jobs for humans will result in less character-building and more podcasts.

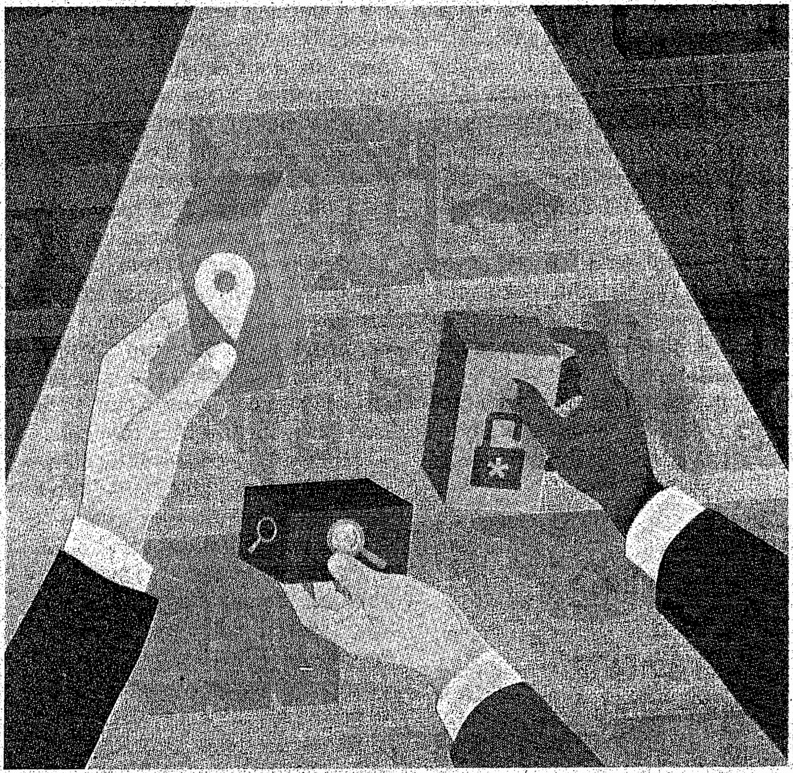
Relish the thought that the phrase "outside the box" will come to mean "human."

Acknowledge that the road to the Singularity will be a bumpy one, with rest stops that are named "the slightly less than Spectacularity," "the Incomprehensibility" and the "Call the IT Guy."

Henry Alford is a humorist and journalist and the author of "And Then We Danced: A Voyage into the Groove," among other books.

U.S. Spy Agencies Know Your Secrets. They Bought Them.

Commercial data brokers are providing the government with personal information that might otherwise require search warrants. Should that be allowed? **By Byron Tau**



MITCH BLUNT

Last November, Michael Morell, a former deputy director of the Central Intelligence Agency, hinted at a big change in how the agency now operates. "The information that is available commercially would kind of knock your socks off," Morell said in an appearance on the NatSecTech podcast. "If we collected it using traditional intelligence methods, it would be top secret-sensitive. And you wouldn't put it in a database, you'd keep it in a safe."

In recent years, U.S. intelligence agencies, the military and even local police departments have gained access to enormous amounts of data through shadowy arrangements with brokers and aggregators. Everything from basic biographical information to consumer preferences to precise hour-by-hour movements can be obtained by government agencies without a warrant.

Most of this data is first collected by commercial entities as part of doing business. Companies acquire consumer names and addresses to ship goods and sell services. They acquire consumer preference data from loyalty programs, purchase history or online search queries. They get geolocation data when they build mobile apps or install roadside safety systems in cars.

But once consumers agree to share information with a corporation, they have no way to monitor what happens to it after it is collected. Many corporations have relationships with data brokers and sell or trade information about their

Please turn to page C4

Government Is Buying the Data of Our Daily Lives

Continued from page C1

customers. And governments have come to realize that such corporate data not only offers a rich trove of valuable information but is available for sale in bulk.

Immigration and Customs Enforcement has used address data sold by utility companies to track down undocumented immigrants. The Secret Service has used geolocation data to fight credit card fraud, while the Drug Enforcement Administration has used it to try to find a kidnapping victim in Mexico. A Department of Homeland Security document revealed that the agency used purchased location data from mobile phones to "identify specific stash houses, suspicious trucking firms in North Carolina, links to Native American Reservations in Arizona, connections in Mexico and Central America which were not known and possible [accomplices] and international links to MS- 13 gang homicides." And one government contractor, as part of a counterintelligence demonstration, used data from the gay-themed dating site Grindr to identify federal employees having sexual liaisons on the clock.

Whatever the U.S. can do with commercial data, foreign governments can do too. Last week, President Biden signed an executive order to prevent certain adversary countries, especially China and Russia, from buying bulk commercial data sets about Americans, including genetic information and personal movement information. But the order didn't address the issue of how the U.S. government itself uses commercial data to get around constitutional protections for civil liberties. That issue is now before Congress as lawmakers consider reauthorizing a key surveillance law, prompting a debate over whether it's appropriate for government and corporate power to become so intertwined.

In January 2022, a group of advisers convened by the U.S. Director of National Intelligence issued a report on the changing nature of intelligence. The report, withheld from the public for nearly a year and a half, concluded that "Today, in a way that [few] Americans seem to understand, and even fewer of them can avoid," governments can purchase "information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection."

Earlier generations of data brokers vacuumed up information from public records like driver's licenses and marriage certificates. But today's internet-enabled consumer technology makes it possible to acquire previously unimaginable kinds of data. Phone apps scan the signal environment around your phone and report back, hourly, about the cell towers, wireless earbuds, Bluetooth speakers and Wi-Fi routers that it encounters.

The National Security Agency recently acknowledged buying internet browsing data from private brokers, and several sources have told me about programs allowing the U.S. to buy access to foreign cell phone networks. Those arrangements are cloaked in secrecy, but the data would allow the U.S. to see who hundreds of millions of people around the world are calling.

Car companies, roadside assistance services and satellite radio companies also collect geolocation data and sell it to brokers, who then resell it to government entities. Even tires can be a vector for surveillance. That little computer readout on your car that tells you the tire pressure is 42 PSI? It operates through a wireless signal from a tiny sensor, and government agencies and private companies have figured out how to use such signals to track people.

While it's unclear how far that capability has penetrated into mass surveillance technology, one Utah company called Blyncsy has put up sensors that collect tire pressure identifiers—data meant to be used for anonymized traffic analysis by highway departments and transportation planners. Blyncsy's CEO Mark Pittman said in an email that the company has not sold its sensors to police or national security entities and has recently discontinued the product.

It's legal for the government to use commercial data in intelligence programs because data brokers have either gotten the consent of consumers to collect their information or have stripped the data of any details that could be traced back to an individual. Much commercially available data doesn't contain explicit personal information.

But the truth is that there are ways to identify people in nearly all anonymized data sets. If you can associate a phone, a computer or a car tire with a daily pattern of behavior or a residential address, it can usually be associated with an individual.

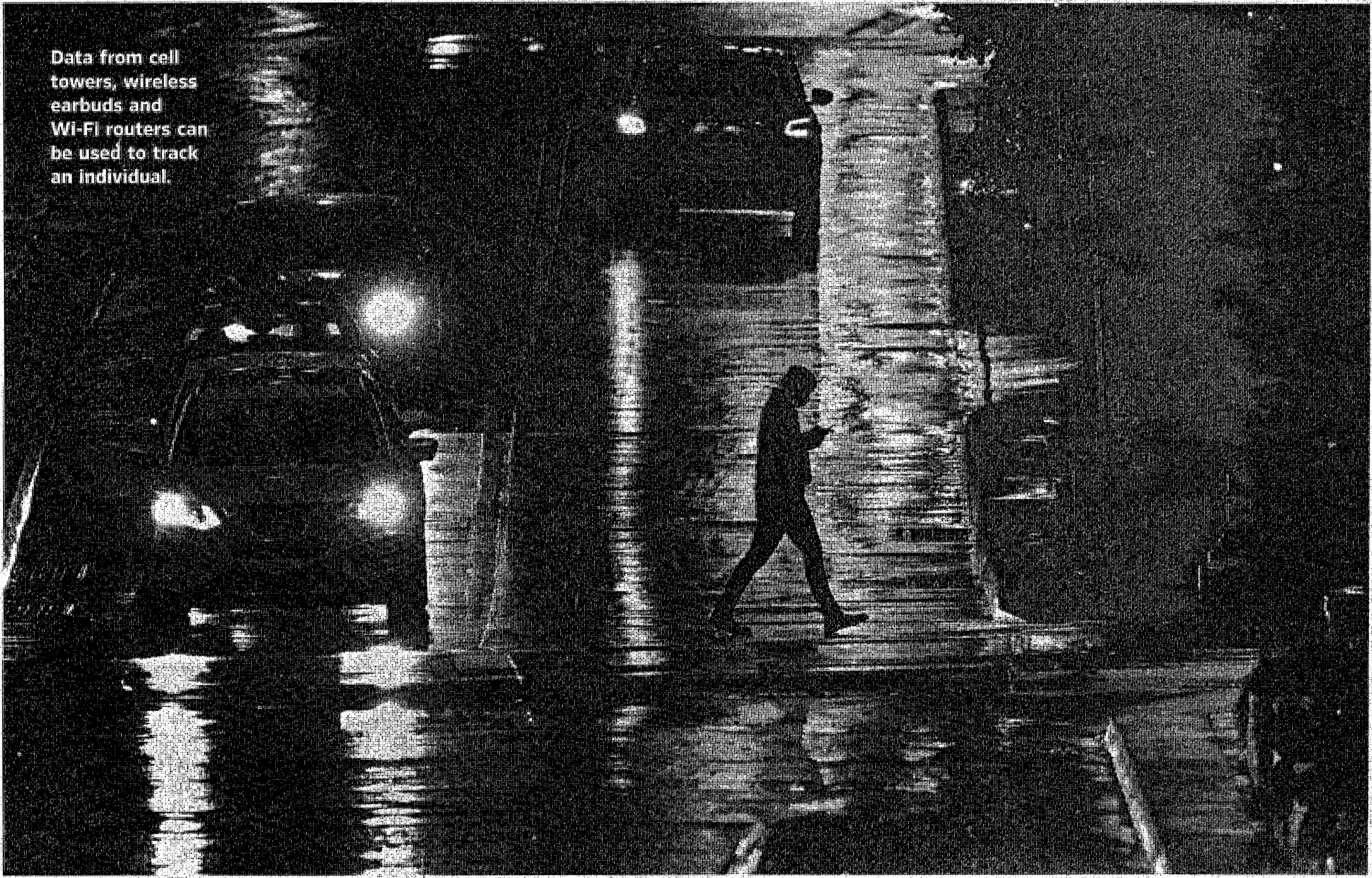
And while consumers have technically consented to the acquisition of their personal data by large corporations, most aren't aware that their data is also flowing to the government, which disguises its purchases of data by working with contractors. One giant defense contractor, Sierra Nevada, set up a marketing company called nContext which is acquiring huge amounts of advertising data from commercial providers. Sierra Nevada and nContext did not respond to a request for comment.

Big data brokers that have reams of consumer information, like LexisNexis and Thomson Reuters, market products to government entities, as do smaller niche players. Companies like Babel Street, Shadowdragon, Flashpoint and Cobwebs have sprung up to sell insights into what happens on social media or other web forums. Location data brokers like Venntel and Safegraph have provided data on the movement of mobile phones.

Car companies sell geolocation data to brokers, who then resell it to government entities.

"Government agencies rely on mobility and location analytics to properly allocate resources and inform critical decisions, including combating human and sex trafficking, identifying food or health deserts, improving infrastructure planning and informing natural disaster preparedness and response," said Jason Sarfati, chief privacy officer of Venntel, in a statement. "Agencies use this data within their approved scope of responsibility and in compliance with the laws under which they were formed."

A group of U.S. lawmakers is trying to stop the government from buying commercial data without deaths continue: Covid will remain a minimize the virus, while other offi- without vaccines would likely have dence over the pandemic period in on the way we live.



Data from cell towers, wireless earbuds and Wi-Fi routers can be used to track an individual.

court authorization by inserting a provision to that effect in a spy law, FISA Section 702, that Congress needs to reauthorize by April 19. The proposal would ban U.S. government agencies from buying data on Americans but would allow law-enforcement agencies and the intelligence community to continue buying data on foreigners. The effort scrambles the usual partisan lines, with support from Republican firebrands like Jim Jordan of Ohio and Andy Biggs of Arizona, as well as liberal Democrats like Ron Wyden of Oregon and Pramila Jayapal of Washington.

But the Biden administration has been lobbying Capitol Hill against the provision. "I would not compare the way that our government uses data to the way that countries of concern are using data," an administration official said last month on a conference call with reporters announcing Biden's executive order. In a bid to convince fellow Democrats to vote against the proposal, Rep. Jim Himes of Connecticut, the top Democrat on the House Intelligence Committee, said that the proposal to ban the purchase of data "would undermine some of the most fundamental and important activities of the intelligence community and law enforcement." House Speaker Mike Johnson, a Republican, pulled the reauthorization bill for the spy law from the floor in February over concerns from intelligence agencies and their allies in Congress, in part because of the proposed restrictions on using commercial data.

Many in the national security establishment think that it makes no sense to ban the government from acquiring data that everyone from the Chinese government to Home Depot can buy on the open market. The data is valuable—in some cases, so valuable that the government won't even discuss what it's buying. "Picture getting a suspect's phone, then in the extraction [of data] being able to see everyplace they'd been in the last 18 months plotted on a map you filter by date ranges," wrote one Maryland state trooper in an email obtained under public records laws. "The success lies in the secrecy."

For spies and police officers alike, it is better for people to remain in the dark about what happens to the data generated by their daily activities—because if it were widely known how much data is collected and who buys it, it wouldn't be such a powerful tool. Criminals might change their behavior. Foreign officials might realize they're being surveilled. Consumers might be more reluctant to uncritically click "I accept" on the terms of service when downloading free apps. And the American public might finally demand that, after decades of inaction, their lawmakers finally do something about unrestrained data collection.

This essay is adapted from Byron Tau's new book, "Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State." A former reporter for The Wall Street Journal, he is now a reporter at NOTUS, a new nonprofit newsroom in Washington, D.C.

CHARLIE RIEDEL/ASSOCIATED PRESS

ABIGAIL DRUMMOND

226-20 129th Ave • Queens, NY 11413 • (718) 807-1255
abigail.drummond22@my.stjohns.edu

EDUCATION

ST. JOHN'S UNIVERSITY SCHOOL OF LAW, Queens, New York
J.D. Candidate, May 2025
Academics: G.P.A.: 3.9
Honors: *Recipient,* Ron Brown Scholarship Program
Recipient, Theodore T. Jones, Jr. Fellowship
Activities: *Editor-in-Chief*, St. John's Law Review
Teaching Assistant, Contracts; Lawyering; Criminal Law
Member, Intellectual Property Law Society
Member, Black Law Students Association
Member, Women's Law Society

PRINCETON UNIVERSITY, Princeton, New Jersey
A.B., in Ecology and Evolutionary Biology, May 2022
Academics: G.P.A.: 3.54
Honors: Sigma Xi
Thesis: "The Epidemic Next Door: A statistical framework for understanding current and future arbovirus outbreak risk"
Certificates*:* Global Health and Health Policy; Statistics and Machine Learning
Activities: *Member,* Global Health Scholars Program
Lead Supervisor, Office of Annual Giving TigerCall

EXPERIENCE

HUGO BOSS, New York, New York
Law Clerk, Spring 2024
Assists corporate counsel in legal research, due diligence, and contract drafting for commercial real estate, cybersecurity and privacy, and intellectual property matters.

T-MOBILE, Parsippany-Troy Hills, New Jersey
Law Clerk, Summer 2023
Assisted corporate counsel in legal research, memo writing, and contract drafting for Business clients across a number of practice areas including tech and cybersecurity, commercial real estate, labor and employment, and transactional law.

NEW YORK YANKEES, Bronx, New York
Part-Time Tour Guide, 2022–Present
Gives tours of Yankee Stadium and acts as an ambassador for the New York Yankees.

TUFTS INSTITUTE FOR GLOBAL OBESITY RESEARCH, Boston, Massachusetts
Research Assistant, Summer 2021
Developed a machine learning-based framework to visualize the socioenvironmental predictors of childhood obesity. Developed an ensemble learning model to predict the prevalence of childhood obesity at the county level.

VOLUNTEER EXPERIENCE

PREP FOR PREP, New York, New York
Facilitator, 2021–Present
Leads Prep for Prep high school students through Aspects of Leadership, a required leadership development curriculum, which focuses on ethical and effective leadership.

ASMA HALIMI

426 Broadway Greenlawn Rd, Huntington, NY 11743
631-860-8998 • Asma.hlco@gmail.com

EDUCATION

St. John's University School of Law, Queens, NY
Juris Doctorate Expected, June 2026
Academics: **GPA:** 3.96
Activities: *1L Representative,* Women's Law Society; *Civil Legal Advice and Resource Office* Coordinator and Volunteer; *Member,* Public Interest Center; *Member*, Intellectual Property Law Society

SUNY College at Old Westbury, Old Westbury, NY
B.A., *magna cum laude*, Politics, Economics, and Law, May 2023
Academics: **GPA:** 3.85
Honors: Dean's List (all semesters); Awarded SUNY Chancellor's Award; President's Award Nominee; Honor's College Member; Departmental Award for Academic Excellence and Service; Published Legislative Report in NYS Assembly Distinguished Intern Report

PROFESSIONAL EXPERIENCE

Enzo BioChem, Inc., Farmingdale, NY
Legal Intern, November 2022 – August 2023
Drafted reports for in-house counsel regarding assignment and termination obligations based on review of lease agreements during the acquisition process of clinical labs division. Worked with compliance officers during regulatory audits and assessed business policies regarding HIPAA compliance and data security. Compiled report of active patents and trademarks for executives and outside counsel to comply with acquisition-related transfer of intellectual property.

New York State Assembly, Albany, NY
Legislative Intern, January 2022 – June 2022
Authored and published a report on healthcare policy and legislation with extended committee deliberation. Collaborated with legislative team to research healthcare policy issues specific to Western New York. Lead daily meetings with interest groups to discuss upcoming legislative initiatives. Drafted resolutions on healthcare and hospice legislation. Worked with constituents on pandemic-era policy information regarding unemployment benefits.

TD Bank, Melville, NY
Teller, July 2021 – December 2021
Regional teller award for exceeding sales quota and consistent growth of personal business portfolio. Opened and processed transactions for personal and business accounts. Proactively educated customers on banking products and services to provide personalized recommendations. Securely processed sensitive customer data and ensured compliance with cash management requirements.

Law Offices of David Okrent, Melville, NY
Legal Office Assistant, June 2019 – December 2021
Conducted phone meetings with clients and estate administrators; assisted in will drafting process; organized and marketed weekly seminars educating the community in eldercare and estate law developments.

SKILLS, INTERESTS & PROFESSIONAL MEMBERSHIPS

Languages: English (Native Fluency), Pashto (Second Language)
Interests: Chess, Poetry, Volunteering (Cat Shelter & Walt Whitman Historical Association)
Memberships: Labor and Employment Relations Association, Federal Bar Association

BYRON C. CHOU

BACKGROUND

Byron C. Chou graduated from Carnegie Mellon University with a Bachelor of Science in Business Administration in 2009, where he was awarded the Sidney M. and Sylvia B. Feldman Memorial Scholarship. Thereafter, Mr. Chou received his Juris Doctor degree from St. John's University School of Law in 2017, where he was recipient of the Kenneth Wang Memorial Scholarship. Mr. Chou has a diversified background in forensic accounting, finance, and business valuation.

Prior to joining Gassman Baiamonte Gruner, P.C., Mr. Chou was a Senior Associate with the firm of Klein Liebman Gresen, LLC, a boutique valuation and litigation support firm located in Melville, NY. During his tenure at KLG, Mr. Chou assisted hundreds of clients, attorneys, and judges in contested and mediated divorce matters by conducting forensic accounting analyses, valuations of publicly or closely-held companies/entities, deferred compensation evaluations (i.e., DeJesus and Majauskas), asset tracings, and enhanced earnings calculations.

Since 2017, Mr. Chou has devoted his practice exclusively to matrimonial and family law where his extensive forensic accounting background is leveraged in litigating high-net worth contested divorces and complex equitable distribution issues, agreements (prenuptial, postnuptial, and separation), child custody, and support issues. He is an active member of the Nassau County Bar Association, the Theodore Roosevelt American Inns of Court, and the New York State Bar Association; additionally, Mr. Chou serves as the Events Coordinator of the Asian American Attorney Section, Chair of the New Lawyers Committee and on the President's Panel of the Nassau County Bar Association. Mr. Chou also serves on the Asian Advisory Council to the Nassau County District Attorney.

A lifelong resident of Long Island, Mr. Chou grew up in Syosset, NY and currently resides in Huntington, NY where he enjoys playing pickleball and spending time with his dog, Mysti.

PROFESSIONAL EXPERIENCE

GASSMAN BAIAMONTE GRUNER, P.C. **August 2017 - Present**
Associate Attorney

KLEIN LIEBMAN & GRESEN, LLC **June 2009 - July 2017**
Senior Forensic Accountant

ADMISSIONS & MEMBERSHIPS

BAR ADMISSION, New York 2nd Dept. **January 2018**

THEODORE ROOSEVELT AMERICAN INN OF COURT **June 2021 – Present**
Barrister Member

NASSAU COUNTY BAR ASSOCIATION **August 2017 - Present**
Chair · New Lawyers' Committee (Current), LGBTQ Committee (2020-2022)
Member · Asian American Attorney Section, Matrimonial Law Committee

EDUCATION & MERIT

ST. JOHN'S UNIVERSITY SCHOOL OF LAW **June 2017**
Juris Doctor
Honors: Kenneth Wang Memorial Scholarship
Leadership: *Senator* · Student Bar Association

CARNEGIE MELLON UNIVERSITY TEPPER SCHOOL OF BUSINESS **May 2009**
Bachelor of Science in Business Administration
Honors: Sidney M. & Sylvia B. Endowed Scholar

Leadership: *President* · Student Dormitory Council
Senator · Undergraduate Student Senate

Leadership and Service Award, Carnegie Mellon University **May 2009**
Nassau County Comptroller's Achievement Award **June 2005**

SPEAKING ENGAGEMENTS

The Modern Family: Marriage and Estate Planning Concerns **March 2019**
Life of a Lawyer: Career Development and Networking **July 2022 & 2023**
Leveraging AI & ChatGPT in the practice of Matrimonial Law **October 2023**

Elizabeth M. Daitz

85 S. Centre Ave #A9, Rockville Centre, NY 11570; cell: 516-652-3880; e-mail: elizabethdaitz@gmail.com

EXPERIENCE

Suffolk County Police Department (SCPD)

Assistant Commissioner of Police, March 2022 – Present

- Position the Suffolk County Police Department to be the nation's most innovative, efficient, effective, and equitable law enforcement organization, serving over 1.5 million county residents across 911 square miles.
- Drive strategic planning, implementation, and innovation. Transform law enforcement operations by holistically enhancing policy, process, technology, training, compliance, data collection, transparency, and accountability to support performance improvement and reduce the administrative burden of policework on the patrol force.
- Achievements include implementing evidence-based patrol strategies to reduce crime and disorder; creating a comprehensive Body Worn Camera and digital evidence management program; supporting discovery compliance; coordinating assets and increasing the role of analytics in operational decision-making through the expansion of the Suffolk Crime Analysis Center; leading efforts to resolve institutional litigation and vacate the agency's consent decree; and creating a culture of compliance designed to support excellence and reduce risk.

New York City Police Department (NYPD)

Executive Director, Strategic Initiatives, September 2020 – March 2022

- Supported all efforts to design and drive long term, enterprise-wide transformation by evaluating policies, programs, and resources, striving toward maximum organizational efficiency and effectiveness. Designed and implemented crime reduction strategies, reduced organizational risk, and enhanced service delivery.
- Lead the NYPD Information Management Task Force. Convened internal stakeholders, local prosecutors, and technologists to develop and execute a comprehensive information management strategy. Enhanced transparency and discovery compliance while reducing costs and freeing up uniform officers to return to patrol functions.

White House Fellow

Office of the Chief of Staff to the President of the United States, August 2019 – August 2020

- Served as Senior Advisor to the Deputy Chief of Staff for Policy Coordination. Appointed as liaison for policy discussion and implementation across the Executive Office of the President (EOP) of the United States.
- Drafted and implemented the President's Executive Order (EO) 13929 "Safe Policing for Safe Communities." Served as White House subject matter expert on police use of force. Coordinated with senior administration officials, the Attorney General, leading law enforcement organizations and community stakeholders to find consensus around accreditation, data, training, hiring, retention, resilience, and community engagement.
- Lead White House representative on multiple lines of effort implementing the Executive Order "Maintaining American Leadership in Artificial Intelligence (AI)," part of a $1 billion federal investment in AI technologies.
- Provided federal support to the state managed and locally executed expansion of COVID-19 testing by aiding in the coordination and delivery of over 12.7 million tests to 54 states and territories.

New York City Police Department (NYPD)

Executive Director, Civil Litigation, June 2018 – August 2019
Director, Civil Matters, June 2014 – June 2018

- Conceptualized, developed and lead the Police Action Litigation Section (PALS), which enhanced the evaluation and defense of civil lawsuits to ensure more just results, leading to a fifty percent decline in lawsuits against the NYPD, contributing to almost $100 million in savings in one fiscal year.
- Used consequential, merits-based litigation data to both improve individual officer performance and enhance NYPD training, policies and procedures. Implemented steps to reverse litigation trends, mitigate the risk of civil litigation, and enhance the quality of law enforcement service delivery.

New York City Law Department, Office of the Corporation Counsel

Senior Counsel, Special Federal Litigation Division, September 2009 – June 2014
Assistant Corporation Counsel, Special Federal Litigation Division, September 2005 – September 2009

- Responsible for all aspects of litigation including pleadings, discovery, motion practice, oral argument, trial, and settlement negotiations in defending the City of New York and its employees in § 1983 federal civil rights actions in the Southern and Eastern Districts of New York.
- Conducted six federal trials, including a fatal police shooting case and consolidated cases brought by over three hundred plaintiffs challenging the constitutionality of NYPD arrest processing policies at demonstrations.

PROFESSIONAL HONORS

- Long Island Arts Council of Freeport, Public Service Award (2023)
- Keynote Speaker, NicheRMS User Group Conference (2023)
- Member, Justice Action Network Foundation Law Enforcement Roundtable (2022-present)
- "On Kindness and Resilience after Sandy," published in *Newsday*, October 27, 2022
- Women in AI Awards, Finalist, AI in Government: AI Disruptor of the Year (2022)
- New York City and State "Above and Beyond" Award (2021)
- "The Best Way Forward: Address the Police Accountability Gap," Published in *The Hill*, April 22, 2021
- Member, NYS Division of Criminal Justice Services Advisory Panel on Use of Force Policy (2015)
- Participant in the New York State Justice Task Force, developing recommendations on "Root Cause Analysis" to prevent wrongful convictions (2015)
- New York City Bar Association Municipal Affairs Award (2011)

EDUCATION

Leading with Impact: Skills for Complex Challenges
Columbia School of International and Public Affairs, Executive Education Program, 2021

Police Management Institute
Columbia Business School, Executive Education Program, Session XXIX, 2017

St. John's University School of Law, Jamaica, New York
Juris Doctor, *cum laude*, June, 2005

Adelphi University Honors College, Garden City, New York
B.A. Degree, *summa cum laude*, in Sociology, Minor: Fine Arts, May 2002

St. Anne's College, Oxford University, Oxford, England
"The Special Relationship Between the United States and Great Britain," Summer 2001

AFFILIATIONS

International Association of Chiefs of Police (IACP)
Police Executive Research Forum (PERF)
National Association of Women Law Enforcement Executives (NAWLEE)
Chiefs of Police Association of Suffolk County (COPASC)
White House Fellows Foundation and Association (WHFFA)
Federalist Society
Theodore Roosevelt American Inn of Court
Admitted to practice law in New York State and the Southern and Eastern Districts of New York

Hon. Ira B. Warshawsky

Of Counsel

990 Stewart Avenue
Garden City, New York 11530
(516) 741-6565
iwarshawsky@msek.com

Practice Areas

Litigation & Dispute Resolution

Professional Responsibility

Alternative Dispute Resolution

Education

Brooklyn Law School
J.D., 1969

Rutgers University
B.A., 1966

Memberships

American Bar Association

New York State Bar Association

New York Bar Foundation, Fellow

Nassau County Bar Association, Former Director; Community Relations & Public Education Committee, and Strategic Planning Committee, former Chairs

Nassau County District Court Judges' Association, Past President

Assistant District Attorneys Association of Nassau County, Past President

Jewish Lawyers Association

Nassau Academy of Law, Former Dean

Theodore Roosevelt American Inn of Court, Member and Past President

American College of Business Court Judges, Founding Member and Past President

Special Masters of Commercial Division, New York County

Admissions

New York State

Justice Ira B. Warshawsky, ret. is Of Counsel in the Litigation and Alternative Dispute Resolution practices at Meyer, Suozzi, English & Klein, P.C. in Garden City, Long Island, N.Y. Since joining the firm, the judge has handled mediations with a concentration in multiple areas including construction, personal injury and business disputes. The Judge serves not only as an advocate, representing clients in commercial litigation, but also as a mediator, arbitrator, litigator, private judge, special master and referee, especially in the area of business disputes and the resolution of electronic discovery (E-Discovery) issues. The Judge is also a member of NAM's arbitration and mediation panels. Judge Warshawsky was a distinguished member of the New York judiciary for 25 years. Immediately prior to joining Meyer Suozzi, he served as a Supreme Court Justice in one of the State's leading trial parts -- the Commercial Division -- where he presided over all manner of business claims and disputes, including business valuation proceedings, corporate and partnership disputes, class actions and complex commercial cases.

Judge Warshawsky started his career in public service as a Legal Aid attorney in 1970 when he was Assistant Chief of the Family Court branch in Queens County. He served as a Nassau County Assistant District Attorney in the District and County Court trial bureaus from 1972 to 1974. Following these four years of prosecution and defense work he became a law secretary, serving judges of the New York State Court of Claims and County Court of Nassau County. In 1987 he was elected to the District Court and served there until 1997. In 1997 he was elected to the Supreme Court of the State of New York where he has presided in a Dedicated Matrimonial Part, a Differentiated Case Management Part and sat in one of the county's three Dedicated Commercial Parts until 2011.

Judge Warshawsky has been active in numerous legal, educational and charitable organizations during his career. The Judge recently served as an expert in New York Law in the Grand Court of the Cayman Islands. He has also served as a lecturer in various areas of commercial, civil and criminal law, most recently in the area of e-discovery and its ethical problems. He frequently lectures for the National Institute of Trial Advocacy (NITA) at Hofstra and Widener Law Schools. The Judge currently serves as a contributing editor of the *Benchbook for Trial Judges* published by the Supreme Court Justices Association of the State of New York. He has served as a member of the Office of Court Administration's Civil Curriculum Committee. In 2010, while still on the bench, he was named the official representative of the New York State Unified Court System to The Sedona Conference®, a leading organization credited with developing rules and concepts which address electronically stored information in litigation. The judge is currently a member of the Advisory Board of The Sedona Conference.

As a judge in the Commercial Division of the Supreme Court, he authored several informative decisions dealing with the discoverability and cost of producing electronic materials as well as determining “fair value” in corporate dissolution matters. He has presented numerous seminars on electronic discovery to practicing lawyers through the ABA, the NYSBA, the Nassau Bar Association and private corporate law forums.

In 1996 Judge Warshawsky was the recipient of EAC's Humanitarian of the Year Award, in 1997 he received the Nassau County Bar Association President's Award, in 2000 he received the Former Assistant District Attorneys Association's Frank A. Gulotta Criminal Justice Award and in 2004, the Nassau Bar Association's Director's Award. He is also past president of the Men of Reform Judaism, the men’s arm of the Union of Reform Judaism, the parent body of the Reform movement of Judaism. In 2013, 2015, and 2016, Judge Warshawsky was voted as one of the top 10 Arbitrators in a *New York Law Journal* reader’s poll. In 2016, he was also named an “ADR Champion” by the *National Law Journal*.

In 2018, Judge Warshawsky was named ADR Champion by The National Law Journal. In 2017, he was given a ProBono Award at the Nassau County Bar Association’s Access to Justice for being one of Nassau’s attorneys to provide the most pro bono hours of service in 2016.

Jess A. Bunshaft

Principal

Synergist Mediation

Jess Bunshaft is mediator & arbitrator, and is a principal of Synergist Mediation, in practice as an attorney for over 32 years and bringing over 19 years of mediation experience to the practice. His experience as a trial lawyer, trying major cases in tort & civil rights matters in both state and federal courts, combined with his experience as a business executive, make him uniquely positioned to handle business disputes, employment matters, tort cases, and a host of other issues found in an active ADR practice.

In addition to his legal and ADR experience, Jess has worked in senior municipal management, as a healthcare system vice president, hospital vice president, and executive vice president of one of the largest not-for-profit organizations in New York.

Recognized for his skill in mediation, Jess:

- Is Past President of the Theodore Roosevelt American Inn of Court
- Is a mediator for the United States District Courts for the Southern District of New York (SDNY) and the Eastern District of New York (EDNY)
- Serves as a Special Master for the Appellate Division, Second Department, of the New York State Supreme Court, in its mandatory mediation program
- Is a member of the Commercial Division mediation panel of the NYS Supreme Court, Nassau County
- Serves on the mediation panels of multiple other New York counties, including Bronx and Richmond counties
- Has led mediator training programs and served as a facilitator for New York State Bar Association commercial mediator training programs
- Created and led in-house employee relations mediation programs, resolving hundreds of employee-management disputes for over 20 years
- Has extensive experience in employment law, tort actions, civil rights matters, business management and commercial litigation
- Has worked as an employee advocate in diverse settings
- Was co-chair the Alternative Dispute Resolution Committee of the Nassau County Bar Association (NCBA)
- Is a member of the House of Delegates of the New York State Bar Association
- Served in the management of hospital/healthcare organizations throughout the New York metro area
- Has taught law students studying mediation, including serving as mediator for the mediation advocacy program at the St. John's University School of Law, for the ABA mediation advocacy competition at Cardozo Law School, and for the FINRA Dispute Resolution Triathlon.
- Co-chaired the 2019 NYSBA/NCBA Advanced Commercial Mediator Training program and taught as a facilitator in the 2020 Basic & Advanced Mediator programs

Jess also is a mediator and arbitrator for Part 137 fee disputes, including chairing panel arbitrations in New York and Bronx counties and as a solo arbitrator in Nassau County, and is an arbitrator for the

Financial Industry Regulatory Authority (FINRA).

With extensive training and over 19 years of experience in mediation, over 20 years of corporate management experience, as well as having served as Nassau County's Senior Trial Attorney in Tort & Civil Rights Litigation, combined with over 30 years of legal practice in a diverse array of specialties, including personal injury, civil rights, labor & employment law, and corporate litigation, Jess brings a broad base of experience and skill now focused on helping parties resolve a variety of matters.

Thomas A. O'Rourke
O'Rourke IP Law P.L.L.C.
425 Broadhollow Rd.
Melville, N. Y. 11747
631-423-2700
TORourke@ORourkeIPLaw.com

Mr. O’Rourke’s practice involves all areas of patent, trademark and copyright law. For over thirty years he has been registered to practice before the United States Patent & Trademark Office. Mr. O’Rourke has counseled clients regarding the procurement and enforcement of patents, trademarks, copyrights and trade secrets in a variety of technologies including mechanical, and computer technology. In addition, his practice involves domestic and international technology transfer, acquisition and licensing. He is a member of the bar of the States of New York and California. He has also been admitted to numerous Federal District Courts and Courts of Appeal across the country including, the Court of Appeals for the Federal Circuit.

Mr. O’Rourke has been a member of the Board of Directors of the New York Intellectual Property Law Association. Mr. O’Rourke has been Chairman of the Suffolk County Bar Association’s Committee on Intellectual Property Law and has been a member of the Advisory Board of the Licensing Journal. He has lectured on Intellectual Property Law at numerous Continuing Legal Education programs, including programs presented by the American Bar Association, the Connecticut Intellectual Property Law Association and the Suffolk County Bar Association. He was also the Editor of the New York Intellectual Property Law Association Bulletin and the author of numerous articles on patents, trademarks and copyrights for the New York Intellectual Property Law Association. Mr. O’Rourke has also authored monthly articles on intellectual property law licensing, which have appeared in the Licensing Journal. Mr. O’Rourke has also been named as a Super Lawyer.

Mr. O’Rourke has a B.S. degree in Chemistry from Fordham University and obtained his J.D. degree from St. John's University School of Law, where he was a member of the Law Review.

VICTORIA CIMINERA

156 George Place, Oceanside, NY 11572 • (516) 368-2221 • victoria.ciminera22@my.stjohns.edu

EDUCATION

ST. JOHN'S UNIVERSITY SCHOOL OF LAW, Queens, NY
Candidate for J.D., May 2025

Honors:	*Staff Member*, *St. John's Law Review*
	Recipient, Aequitas Diversity Scholarship
	Dean's List (Fall 2022, Spring 2023, Fall 2023)
	Corporate Law Firm Alliance Summer Program Fellow (CLASP), LatinoJustice
	Dean's Award for Excellence, Employment Discrimination (Fall 2023)
Activities:	*Vice President,* Labor Relations and Employment Law Society (LRELS)
	Co-Director of Events, Latin American Law Students Association (LALSA)
	Teaching Assistant, Introduction to Law (Fall 2023)
	Teaching Assistant, Legal Writing I (Fall 2023) & Legal Writing II (Spring 2024)
	Student Ambassador, The Theodore Roosevelt American Inn of Court
Publications:	"Emojis go to Court — No LOLing in the Workplace"
	(http://stjclelblog.org/2023/01/emojis-go-to-court-no-loling-in-the-workplace/)
	"Truth Hurts – Is Lizzo 100% THAT Employer"
	(https://stjclelblog.org/2023/08/truth-hurts-is-lizzo-100-that-employer/)

MOLLOY UNIVERSITY, Rockville Centre, NY
B.A., *summa cum laude,* Philosophy & Political Science, May 2022

Minor:	Legal Studies
G.P.A.:	3.95
Honors:	Dean's List (eight consecutive semesters)
	Liberal Arts Honors Program
	Departmental Honors Award (Philosophy)
	Phi Sigma Tau (Philosophy Honor Society)
	Pi Sigma Alpha (Political Science Honor Society)
	Lambda Epsilon Chi (Legal Studies Honor Society)
Activities:	Global Citizenship Alliance, Salzburg, Austria (June 2019)

LEGAL EXPERIENCE

METLIFE, New York, NY
Law Clerk, May 2023 – July 2023
Performed research on state statutes and regulations to ensure MetLife's compliance. Completed writing assignments including a legal memorandum for the litigation department. Reviewed contracts and power of attorney documents.

NEW YORK STATE DIVISION OF HUMAN RIGHTS, Hempstead, NY
Student Intern, January 2022 – April 2022
Conducted fact finding interviews with complainants and respondents. Drafted final investigative reports to determine a cause of action for workplace discrimination cases.

OTHER EXPERIENCE

DANCE INNOVATIONS INC., Oceanside, NY
Dance Instructor, September 2017 – August 2022
Instructed, choreographed, and assisted with dance classes of various styles for preschool to high school age students.

ADDITIONAL INFORMATION

ABA Paralegal Certification (Molloy University 2022)
Cada Voto Cuenta Volunteer Event (LatinoJustice 2023)