JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA24-317A

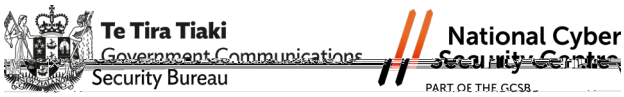
November 12, 2024






Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité



2023 Top Routinely Exploited Vulnerabilities

Summary

The following cybersecurity agencies coauthored this joint Cybersecurity Advisory (hereafter collectively referred to as the authoring agencies):

- **United States:** The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and National Security Agency (NSA)
- **Australia:** Australian Signals Directorate's Australian Cyber Security Centre (ACSC)
- **Canada:** Canadian Centre for Cyber Security (CCCS)
- **New Zealand:** New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team New Zealand (CERT NZ)
- **United Kingdom:** National Cyber Security Centre (NCSC-UK)

This advisory provides details, collected and compiled by the authoring agencies, on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2023 and their associated Common Weakness Enumerations (CWEs). Malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks in 2023 compared to 2022, allowing them to conduct operations against high priority targets.

The authoring agencies strongly encourage vendors, designers, developers, and end-user organizations to implement the following recommendations, and those found within the **Mitigations** section of this advisory, to reduce the risk of compromise by malicious cyber actors.

- **Vendors, designers, and developers**. Implement secure by design and default principles and tactics to reduce the prevalence of vulnerabilities in your software.
  - **Follow the SP 800-218 Secure Software Development Framework (SSDF)** and implement secure by design practices into each stage of the software development life cycle (SDLC). Establish a coordinated vulnerability disclosure program that includes processes to determine root causes of discovered vulnerabilities.

- **Prioritize secure by default configurations**, such as eliminating default passwords and not requiring additional configuration changes to enhance product security.
- Ensure that published CVEs include the proper CWE field, identifying the root cause of the vulnerability.

- **End-user organizations:**
  - **Apply timely patches to systems.**
    Note: If CVEs identified in this advisory have not been patched, check for signs of compromise before patching.
  - **Implement a centralized patch management system.**
  - Use security tools such as endpoint detection and response (EDR), web application firewalls, and network protocol analyzers.
  - **Ask your software providers to discuss their secure by design program**, provide links to information about how they are working to remove classes of vulnerabilities, and to set secure default settings.

Table of Contents

Summary 1
Purpose 4
Technical Details 4
Key Findings 4
Cybersecurity Efforts to Include 4
Top Routinely Exploited Vulnerabilities 4
Additional Routinely Exploited Vulnerabilities 9
Mitigations 13
Vendors and Developers 13
End-User Organizations 14
Vulnerability and Configuration Management 14
Identity and Access Management 15
Protective Controls and Architecture 15
Supply Chain Security 16
Resources 16
References 17
Reporting 17
Disclaimer 17
Version History 17
Appendix: Patch Information and Additional Resources for Top Exploited Vulnerabilities 18

Purpose

The authoring agencies developed this document in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

Technical Details

Key Findings

In 2023, malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks compared to 2022, allowing them to conduct cyber operations against higher-priority targets. In 2023, the majority of the most frequently exploited vulnerabilities were initially exploited as a zero-day, which is an increase from 2022, when less than half of the top exploited vulnerabilities were exploited as a zero-day.

Malicious cyber actors continue to have the most success exploiting vulnerabilities within two years after public disclosure of the vulnerability. The utility of these vulnerabilities declines over time as more systems are patched or replaced. Malicious cyber actors find less utility from zero-day exploits when international cybersecurity efforts reduce the lifespan of zero-day vulnerabilities.

Cybersecurity Efforts to Include

Implementing security-centered product development lifecycles. Software developers deploying patches to fix software vulnerabilities is often a lengthy and expensive process, particularly for zero-days. The use of more robust testing environments and implementing threat modeling throughout the product development lifecycle will likely reduce overall product vulnerabilities.

Increasing incentives for responsible vulnerability disclosure. Global efforts to reduce barriers to responsible vulnerability disclosure could restrict the utility of zero-day exploits used by malicious cyber actors. For example, instituting vulnerability reporting bug bounty programs that allow researchers to receive compensation and recognition for their contributions to vulnerability research may boost disclosures.

Using sophisticated endpoint detection and response (EDR) tools. End users leveraging EDR solutions may improve the detection rate of zero-day exploits. Most zero-day exploits, including at least three of the top 15 vulnerabilities from last year, have been discovered when an end user or EDR system reports suspicious activity or unusual device malfunctions.

Top Routinely Exploited Vulnerabilities

Listed in **Table 1** are the top 15 vulnerabilities the authoring agencies observed malicious cyber actors routinely exploiting in 2023 with details also discussed below.

- CVE-2023-3519: This vulnerability affects Citrix NetScaler ADC and NetScaler Gateway.
  - Allows an unauthenticated user to cause a stack buffer overflow in the NSPPE process by using a HTTP GET request.
- CVE-2023-4966: This vulnerability affects Citrix NetScaler ADC and NetScaler Gateway.
  - Allows session token leakage; a proof-of-concept for this exploit was revealed in October 2023.

- CVE-2023-20198: This vulnerability affects Cisco IOS XE Web UI.
  - Allows unauthorized users to gain initial access and issue a command to create a local user and password combination, resulting in the ability to log in with normal user access.
- CVE-2023-20273: This vulnerability affects Cisco IOS XE, following activity from CVE-2023-20198.
  - Allows privilege escalation, once a local user has been created, to root privileges.
- CVE-2023-27997: This vulnerability affects Fortinet FortiOS and FortiProxy SSL-VPN.
  - Allows a remote user to craft specific requests to execute arbitrary code or commands.
- CVE-2023-34362: This vulnerability affects Progress MOVEit Transfer.
  - Allows abuse of an SQL injection vulnerability to obtain a sysadmin API access token.
  - Allows a malicious cyber actor to obtain remote code execution via this access by abusing a deserialization call.
- CVE-2023-22515: This vulnerability affects Atlassian Confluence Data Center and Server.
  - Allows exploit of an improper input validation issue.
    - Arbitrary HTTP parameters can be translated into getter/setter sequences via the XWorks2 middleware and, in turn, allow Java objects to be modified at run time.
    - The exploit creates a new administrator user and uploads a malicious plugin to get arbitrary code execution.
- CVE-2021-44228: This vulnerability, known as Log4Shell, affects Apache's Log4j library, an open source logging framework incorporated into thousands of products worldwide.
  - Allows the execution of arbitrary code.
    - An actor can exploit this vulnerability by submitting a specially crafted request to a vulnerable system, causing the execution of arbitrary code.
    - The request allows a cyber actor to take full control of a system.
    - The actor can then steal information, launch ransomware, or conduct other malicious activity.
    - Malicious cyber actors began exploiting the vulnerability after it was publicly disclosed in December 2021.
- CVE-2023-2868: This is a remote command injection vulnerability that affects the Barracuda Networks Email Security Gateway (ESG) Appliance.
  - Allows an individual to obtain unauthorized access and remotely execute system commands via the ESG appliance.
- CVE-2022-47966: This is an unauthenticated remote code execution vulnerability that affects multiple products using Zoho ManageEngine.
  - Allows an unauthenticated user to execute arbitrary code by providing a crafted samlResponse XML to the ServiceDesk Plus SAML endpoint.
- CVE-2023-27350: This vulnerability affects PaperCut MF/NG.
  - Allows a malicious cyber actor to chain an authentication bypass vulnerability with the abuse of built-in scripting functionality to execute code.

- CVE-2020-1472: This vulnerability affects Microsoft Netlogon.
  - Allows privilege escalation.
    - An unauthorized user may use non-default configurations to establish a vulnerable Netlogon secure channel connection to a domain controller by using the Netlogon Remote Protocol.
      Note: This CVE has been included in top routinely exploited vulnerabilities lists since 2021.
- CVE-2023-42793: This vulnerability can affect JetBrains TeamCity servers.
  - Allows authentication bypass that allows remote code execution against vulnerable JetBrains TeamCity servers.
- CVE-2023-23397: This vulnerability affects Microsoft Office Outlook.
  - Allows elevation of privilege.
    - A threat actor can send a specially crafted email that the Outlook client will automatically trigger when Outlook processes it.
    - This exploit occurs even without user interaction.
- CVE-2023-49103: This vulnerability affects ownCloud graphapi.
  - Allows unauthenticated information disclosure.
    - An unauthenticated user can access sensitive data such as admin passwords, mail server credentials, and license keys.

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2023

CVE	Vendor	Product(s)	Vulnerability Type	CWE
CVE-2023-3519	Citrix	NetScaler ADC NetScaler Gateway	Code Injection	CWE-94: Improper Control of Generation of Code ('Code Injection')
CVE-2023-4966	Citrix	NetScaler ADC NetScaler Gateway	Buffer Overflow	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2023-20198	Cisco	IOS XE Web UI	Privilege Escalation	CWE-420: Unprotected Alternate Channel

CVE	Vendor	Product(s)	Vulnerability Type	CWE
CVE-2023-20273	Cisco	IOS XE	Web UI Command Injection	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CVE-2023-27997	Fortinet	FortiOS FortiProxy SSL-VPN	Heap-Based Buffer Overflow	CWE-787: Out-of-bounds Write CWE-122: Heap-based Buffer Overflow
CVE-2023-34362	Progress	MOVEit Transfer	SQL Injection	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CVE-2023-22515	Atlassian	Confluence Data Center and Server	Broken Access Control	CWE-20 Improper Input Validation
CVE-2021-44228 (Log4Shell)	Apache	Log4j2	Remote Code Execution (RCE)	CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') CWE-502: Deserialization of Untrusted Data CWE-20 Improper Input Validation CWE-400 Uncontrolled Resource Consumption

CVE	Vendor	Product(s)	Vulnerability Type	CWE
CVE-2023-2868	Barracuda Networks	ESG Appliance	Improper Input Validation	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') CWE-20: Improper Input Validation
CVE-2022-47966	Zoho	ManageEngine Multiple Products	Remote Code Execution	CWE-20 Improper Input Validation
CVE-2023-27350	PaperCut	MF/NG	Improper Access Control	CWE-284: Improper Access Control
CVE-2020-1472	Microsoft	Netlogon	Privilege Escalation	CWE-330: Use of Insufficiently Random Values
CVE-2023-42793	JetBrains	TeamCity	Authentication Bypass	CWE-288: Authentication Bypass Using an Alternate Path or Channel
CVE-2023-23397	Microsoft	Office Outlook	Privilege Escalation	CWE-294: Authentication Bypass by Capture-replay CWE-20: Improper Input Validation
CVE-2023-49103	ownCloud	graphapi	Information Disclosure	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Additional Routinely Exploited Vulnerabilities

The authoring agencies identified other vulnerabilities, listed in **Table 2**, that malicious cyber actors also routinely exploited in 2023—in addition to the 15 vulnerabilities listed in **Table 1**.

Table 2: Additional Routinely Exploited Vulnerabilities in 2023

CVE	Vendor	Product	Vulnerability Type	CWE
CVE-2023-22518	Atlassian	Confluence Data Center and Server	Improper Authorization	CWE-863: Incorrect Authorization
CVE-2023-29492	Novi	Novi Survey	Insecure Deserialization	CWE-94 Improper Control of Generation of Code ('Code Injection')
CVE-2021-27860	FatPipe	WARP, IPVPN, and MPVPN	Configuration Upload Exploit	CWE-434: Unrestricted Upload of File with Dangerous Type
CVE-2021-40539	Zoho	ManageEngine ADSelfService Plus	Authentication Bypass	CWE-706: Use of Incorrectly-Resolved Name or Reference
CVE-2023-0669	Fortra	GoAnywhere MFT	RCE	CWE-502: Deserialization of Untrusted Data
CVE-2021-22986	F5	BIG-IP and BIG-IQ Centralized Management iControl REST	RCE	CWE-918: Server-Side Request Forgery (SSRF)
CVE-2019-0708	Microsoft	Remote Desktop Services	RCE	CWE-416: Use After Free
CVE-2018-13379	Fortinet	FortiOS SSL VPN	Path Traversal	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVE	Vendor	Product	Vulnerability Type	CWE
CVE-2022-31199	Netwrix	Auditor	Insecure Object Deserialization	CWE-502: Deserialization of Untrusted Data
CVE-2023-35078	Ivanti	Endpoint Manager Mobile	Authentication Bypass	CWE-287: Improper Authentication
CVE-2023-35081	Ivanti	Endpoint Manager Mobile (EPMM)	Path Traversal	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVE-2023-44487	N/A	HTTP/2	Rapid Reset Attack	CWE-400: Uncontrolled Resource Consumption
CVE-2023-36844	Juniper	Junos OS EX Series PHP	External Variable Modification	CWE-473: PHP External Variable Modification
CVE-2023-36845	Juniper	Junos OS EX Series and SRX Series PHP	External Variable Modification	CWE-473: PHP External Variable Modification
CVE-2023-36846	Juniper	Junos OS SRX Series	Missing Authentication for Critical Function	CWE-306: Missing Authentication for Critical Function
CVE-2023-36847	Juniper	Junos OS EX Series	Missing Authentication for Critical Function	CWE-306: Missing Authentication for Critical Function
CVE-2023-41064	Apple	iOS, iPadOS, and macOS ImageIO	Buffer Overflow	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CVE-2023-41061	Apple	Apple iOS, iPadOS, and watchOS Wallet	Code Execution	CWE-20 Improper Input Validation

CVE	Vendor	Product	Vulnerability Type	CWE
CVE-2021-22205	GitLab	Community and Enterprise Editions	RCE	CWE-94: Improper Control of Generation of Code ('Code Injection')
CVE-2019-11510	Ivanti	Pulse Connect Secure	Arbitrary File Read	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVE-2023-6448	Unitronics	Vision PLC and HMI	Insecure Default Password	CWE-798: Use of Hard-coded Credentials CWE-1188: Initialization of a Resource with an Insecure Default
CVE-2017-6742	Cisco	IOS and IOS XE Software SNMP	RCE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2021-4034	Red Hat	Polkit	Out-of-Bounds Read and Write	CWE-125: Out-of-bounds Read CWE-787: Out-of-bounds Write
CVE-2021-26084	Atlassian	Confluence Server and Data Center	Object-Graph Navigation Language (OGNL) Injection	CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
CVE-2021-33044	Dahua	Various products	Authentication Bypass	CWE-287: Improper Authentication

CVE	Vendor	Product	Vulnerability Type	CWE
CVE-2021-33045	Dahua	Various products	Authentication Bypass	CWE-287: Improper Authentication
CVE-2022-3236	Sophos	Firewall	Code Injection	CWE-94: Improper Control of Generation of Code ('Code Injection')
CVE-2022-26134	Atlassian	Confluence Server and Data Center	RCE	CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
CVE-2022-41040	Microsoft	Exchange Server	Server-Side Request Forgery	CWE-918: Server-Side Request Forgery (SSRF)
CVE-2023-38831	RARLAB	WinRAR	Code Execution	CWE-345: Insufficient Verification of Data Authenticity CWE-351: Insufficient Type Distinction
CVE-2019-18935	Progress Telerik	Progress Telerik UI for ASP.NET AJAX	Deserialization of Untrusted Data	CWE-502: Deserialization of Untrusted Data
CVE-2021-34473	Microsoft	Microsoft Exchange Server	RCE	CWE-918: Server-Side Request Forgery (SSRF)

Mitigations

Vendors and Developers

The authoring agencies recommend vendors and developers take the following steps to help ensure their products are secure by design and default:

- **Identify repeatedly exploited classes of vulnerability.**
  - Perform an analysis of both CVEs and known exploited vulnerabilities (KEVs) to understand which classes of vulnerability are identified more than others.
  - Implement appropriate mitigations to eliminate those classes of vulnerability.
  - If a product has several instances of SQL injection vulnerabilities, ensure all database queries in the product use parameterized queries and prohibit other forms of queries.
- Ensure business leaders are responsible for security.
  - Business leaders should ensure their teams take proactive steps to eliminate entire classes of security vulnerabilities, rather than only making one-off patches when new vulnerabilities are discovered.
- **Follow SP 800-218 SSDF** and implement secure by design practices into each stage of the SDLC; in particular, aim to perform the following SSDF recommendations:
  - Prioritize the use of memory safe languages wherever possible [SSDF PW 6.1].
  - Exercise due diligence when selecting software components (e.g., software libraries, modules, middleware, frameworks) to ensure robust security in consumer software products [SSDF PW 4.1].
  - Set up secure software development team practices—this includes conducting peer code reviews, working to a common organization secure coding standard, and maintaining awareness of language-specific security concerns [SSDF PW.5.1, PW.7.1, PW.7.2].
  - Establish a vulnerability disclosure program to verify and resolve security vulnerabilities disclosed by people who may be internal or external to the organization [SSDF RV.1.3] and establish processes to determine root causes of discovered vulnerabilities.
  - Use static and dynamic application security testing (SAST/DAST) tools to analyze product source code and application behavior to detect error-prone practices [SSDF PW.7.2, PW.8.2].
- **Configure production-ready products to have the most secure settings by default** and provide guidance on the risks of changing each setting [SSDF PW.9.1, PW9.2].
  - Prioritize secure by default configurations such as eliminating default passwords, implementing single sign on (SSO) technology via modern open standards, and providing high-quality audit logs to customers with no additional configuration necessary and at no extra charge.
- **Ensure published CVEs include the proper CWE field** identifying the root cause of the vulnerability to enable industry-wide analysis of software security and design flaws.

For more information on designing secure by design and default products, including additional recommended secure by default configurations, see CISA's joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default.

End-User Organizations

The authoring agencies recommend end-user organizations implement the mitigations below to improve their cybersecurity posture based on threat actors' activity. 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 CPGs webpage for more information on CPGs, including additional recommended baseline protections.

Vulnerability and Configuration Management

- **Update software, operating systems, applications, and firmware on IT network assets in a timely manner** [CPG 1.E].
  - Prioritize patching KEVs, especially those CVEs identified in this advisory, then critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
  - For patch information on CVEs identified in this advisory, refer to the **Appendix: Patch Information and Additional Resources for Top Exploited Vulnerabilities**.
    - If a patch for a KEV or critical vulnerability cannot be quickly applied, implement vendor-approved workarounds.
    - Replace end-of-life software (i.e., software no longer supported by the vendor).
- **Routinely perform automated asset discovery** across the entire estate to identify and catalogue all the systems, services, hardware, and software.
- **Implement a robust patch management process** and centralized patch management system that establishes prioritization of patch applications [CPG 1.A].
  - Organizations that are unable to perform rapid scanning and patching of internet-facing systems should consider moving these services to mature, reputable cloud service providers (CSPs) or other managed service providers (MSPs).
  - Reputable MSPs can patch applications (such as webmail, file storage, file sharing, chat, and other employee collaboration tools) for their customers.
    Note: MSPs and CSPs can expand their customer's attack surface and may introduce unanticipated risks, so organizations should proactively collaborate with their MSPs and CSPs to jointly reduce risk [CPG 1.F]. For more information and guidance, see the following resources:
    - CISA Insights' Risk Considerations for MSP Customers.

- CISA Insights' Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses.
- ACSC's How to Manage Your Security When Engaging a MSP.

- Document secure baseline configurations for all IT/OT components, including cloud infrastructure.
  - Monitor, examine, and document any deviations from the initial secure baseline [CPG 2.O].
- **Perform regular secure system backups** and create known good copies of all device configurations for repairs and/or restoration.
  - Store copies off-network in physically secure locations and test regularly [CPG 2.R].
- **Maintain an updated cybersecurity incident response plan** that is tested at least annually and updated within a risk informed time frame to ensure its effectiveness [CPG 2.S].

Identity and Access Management

- **Enforce phishing-resistant multifactor authentication (MFA) for all users** without exception [CPG 2.H].
- Enforce MFA on all VPN connections.
  - If MFA is unavailable, require employees engaging in remote work to use strong passwords [CPG 2.A, 2.B, 2.C, 2.D, 2.G].
- **Regularly review, validate, or remove unprivileged accounts** (annually at a minimum) [CPG 2.D, 2.E].
- **Configure access control under the principle of least privilege** [CPG 2.O].
  - Ensure software service accounts only provide necessary permissions (least privilege) to perform intended functions (using non-administrative privileges where feasible).
    Note: See CISA's Capacity Enhancement Guide – Implementing Strong Authentication and ACSC's guidance on Implementing MFA for more information on authentication system hardening.

Protective Controls and Architecture

- **Properly configure and secure internet-facing network devices**, disable unused or unnecessary network ports and protocols, encrypt network traffic, and disable unused network services and devices [CPG 2.V, 2.W, 2.X].
  - Harden commonly exploited enterprise network services, including Link-Local Multicast Name Resolution (LLMNR) protocol, Remote Desktop Protocol (RDP), Common Internet File System (CIFS), Active Directory, and OpenLDAP.
  - Manage Windows Key Distribution Center (KDC) accounts (e.g., KRBTGT) to minimize Golden Ticket attacks and Kerberoasting.
  - Strictly control the use of native scripting applications, such as command-line, PowerShell, WinRM, Windows Management Instrumentation (WMI), and Distributed Component Object Model (DCOM).

- **Implement Zero Trust Network Architecture (ZTNA)** to limit or block lateral movement by controlling access to applications, devices, and databases. Use private virtual local area networks [CPG 2.F, 2.X].
  Note: See CISA's Zero Trust Maturity Model and the Department of Defense's Zero Trust Reference Architecture for additional information on Zero Trust.
- **Continuously monitor the attack surface** and investigate abnormal activity that may indicate cyber actor or malware lateral movement [CPG 2.T].
  - Use security tools, such as endpoint detection and response (EDR) and security information and event management (SIEM) tools.
    - Consider using an information technology asset management (ITAM) solution to ensure EDR, SIEM, vulnerability scanners, and other similar tools are reporting the same number of assets [CPG 2.T, 2.V].
  - Use web application firewalls to monitor and filter web traffic.
    - These tools are commercially available via hardware, software, and cloud-based solutions, and may detect and mitigate exploitation attempts where a cyber actor sends a malicious web request to an unpatched device [CPG 2.B, 2.F].
  - Implement an administrative policy and/or automated process configured to monitor unwanted hardware, software, or programs against an allowlist with specified, approved versions [CPG 2.Q].

Supply Chain Security

- **Reduce third-party applications and unique system/application builds**—provide exceptions only if required to support business critical functions [CPG 2.Q].
- Ensure contracts require vendors and/or third-party service providers to:
  - Provide notification of security incidents and vulnerabilities within a risk informed time frame [CPG 1.G, 1.H, 1.I].
  - Supply a Software Bill of Materials (SBOM) with all products to enhance vulnerability monitoring and to help reduce time to respond to identified vulnerabilities [CPG 4.B].
- **Ask your software providers to discuss their secure by design program,** provide links to information about how they are working to remove classes of vulnerabilities, and to set secure default settings.

Resources

- For information on the top vulnerabilities routinely exploited in 2016–2019, 2020, 2021, and 2022:
  - Joint CSA Top 10 Routinely Exploited Vulnerabilities.
  - Joint CSA Top Routinely Exploited Vulnerabilities.
  - Joint CSA 2021 Top Routinely Exploited Vulnerabilities.
  - Joint CSA 2022 Top Routinely Exploited Vulnerabilities.
- See the **Appendix** for additional partner resources on the vulnerabilities mentioned in this advisory.

- See ACSC's Essential Eight Maturity Model for additional mitigations.
- See ACSC's Cyber Supply Chain Risk Management for additional considerations and advice.

References

- Apache Log4j Vulnerability Guidance

Reporting

U.S. organizations: All organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's CyWatch at (855) 292-3937 or CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations: Report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: Report a significant cyber security incident at gov.uk/report-cyber (monitored 24 hours).

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA, FBI, NSA, ACSC, CCCS, NCSC-NZ, CERT NZ, and NCSC-UK do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring.

Version History

November 12, 2024: Initial version.

Appendix: Patch Information and Additional Resources for Top Exploited Vulnerabilities

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2023-3519	Citrix	**NetScaler ADC and NetScaler Gateway:** 13.1 before 13.1-49.13 13.0 before 13.0-91.13 **NetScaler ADC:** 13.1-FIPS before 13.1-37.159 12.1-FIPS before 12.1-55.297 12.1-NDcPP before 12.1-55.297	Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467	Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells Critical Security Update for NetScaler ADC and NetScaler Gateway
CVE-2023-4966	Citrix	**NetScaler ADC and NetScaler Gateway:** 14.1 before 14.1-8.50 13.1 before 13.1-49.15 13.0 before 13.0-92.19 **NetScaler ADC:** 13.1-FIPS before 13.1-37.164 12.1-FIPS before 12.1-55.300 12.1-NDcPP before 12.1-55.300	NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967	#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability Critical Security Update for NetScaler ADC and NetScaler Gateway
CVE-2023-20198	Cisco	Any Cisco IOS XE Software with web UI feature enabled	Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature	Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2023-27997	Fortinet	**FortiOS-6K7K versions:** 7.0.10, 7.0.5, 6.4.12 6.4.10, 6.4.8, 6.4.6, 6.4.2 6.2.9 through 6.2.13 6.2.6 through 6.2.7 6.2.4 6.0.12 through 6.0.16 6.0.10	Heap buffer overflow in sslvpn pre-authentication	
CVE-2023-34362	Progress	**MOVEit Transfer:** 2023.0.0 (15.0) 2022.1.x (14.1) 2022.0.x (14.0) 2021.1.x (13.1) 2021.0.x (13.0) 2020.1.x (12.1) 2020.0.x (12.0) or older MOVEit Cloud	MOVEit Transfer Critical Vulnerability	#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability
CVE-2023-22515	Atlassian	8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4 8.1.0, 8.1.1, 8.1.3, 8.1.4 8.2.0, 8.2.1, 8.2.2, 8.2.38.3.0, 8.3.1, 8.3.2	Broken Access Control Vulnerability in Confluence Data Center and Server	Threat Actors Exploit Atlassian Confluence CVE-2023-22515 for Initial Access to Networks

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
		8.4.0, 8.4.1, 8.4.28.5.0, 8.5.1		
CVE-2021- 44228 (Log4Shell)	Apache	Log4j, all versions from 2.0-beta9 to 2.14.1 For other affected vendors and products, see CISA's GitHub repository.	Apache Log4j Security Vulnerabilities For additional information, see joint advisory: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities	Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
CVE-2023-2868	Barracuda Networks	5.1.3.001 through 9.2.0.006	Barracuda Email Security Gateway Appliance (ESG) Vulnerability	
CVE-2022-47966	Zoho	Multiple products, multiple versions. (For more details, see Security advisory for remote code execution vulnerability in multiple ManageEngine products)	Security advisory for remote code execution vulnerability in multiple ManageEngine products	
CVE-2023-27350	PaperCut	**PaperCut MF or NG version 8.0 or later (excluding patched versions) on all OS platforms. This includes:** version 8.0.0 to 19.2.7 (inclusive) version 20.0.0 to 20.1.6 (inclusive)	URGENT MF/NG vulnerability bulletin (March 2023)	Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
		version 21.0.0 to 21.2.10 (inclusive) version 22.0.0 to 22.0.8 (inclusive)		
CVE-2020-1472	Microsoft	Netlogon	Netlogon Elevation of Privilege Vulnerability	Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure
CVE-2023-23397	Microsoft	Outlook	Microsoft Outlook Elevation of Privilege Vulnerability	Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations
CVE-2023-49103	ownCloud	graphapi	Disclosure of Sensitive Credentials and Configuration in Containerized Deployments	
CVE-2023-20273	Cisco	Cisco IOS XE Software with web UI feature enabled	Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature	Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2023-42793	JetBrains	In JetBrains TeamCity before 2023.05.4	CVE-2023-42793 Vulnerability in TeamCity: Post-Mortem	Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally
CVE-2023-22518	Atlassian	All versions of Confluence Data Cetner and Confluence Server	Improper Authorization in Confluence Data Center and Server	
CVE-2023-29492	—	—	—	
CVE-2021-27860	FatPipe	WARP, MPVPN, IPVPN 10.1.2 and 10.2.2	FatPipe CVE List	
CVE-2021-40539	Zoho	ManageEngine ADSelfService Plus builds up to 6113	Security advisory - ADSelfService Plus authentication bypass vulnerability	**ACSC Alert:** Critical vulnerability in ManageEngine ADSelfService Plus exploited by cyber actors

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2023-0669	Fortra	GoAnywhere versions 2.3 through 7.1.2	Fortra deserialization RCE	#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability
CVE-2021-22986	F5	**BIG-IP versions:** 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, 14.1.x before 14.1.4, 13.1.x before 13.1.3.6, and 12.1.x before 12.1.5.3 and BIG-IQ 7.1.0.x before 7.1.0.3 and 7.0.0.x before 7.0.0.2	K03009991: iControl REST unauthenticated remote command execution vulnerability CVE-2021-22986	
CVE-2019-0708	Microsoft	Remote Desktop Services	Remote Desktop Services Remote Code Execution Vulnerability	
CVE-2018-13379	Fortinet	FortiOS and FortiProxy 2.0.2, 2.0.1, 2.0.0, 1.2.8, 1.2.7, 1.2.6, 1.2.5, 1.2.4, 1.2.3, 1.2.2, 1.2.1, 1.2.0, 1.1.6	FortiProxy - system file leak through SSL VPN special crafted HTTP resource requests	
CVE-2023-35078	Ivanti	**All supported versions of Endpoint Manager Mobile (EPMM), including:** Version 11.4 releases 11.10, 11.9 and 11.8	CVE-2023-35078 - New Ivanti EPMM Vulnerability	Threat Actors Exploiting Ivanti EPMM Vulnerabilities

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2023-35081	Ivanti	All supported versions of Endpoint Manager Mobile (EPMM), including 11.10, 11.9 and 11.8	CVE-2023-35081 - Remote Arbitrary File Write	Threat Actors Exploiting Ivanti EPMM Vulnerabilities
CVE-2023-36844	Juniper	**Juniper Networks Junos OS on SRX Series and EX Series:** All versions prior to 20.4R3-S9; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S7; 21.3 versions prior to 21.3R3-S5; 21.4 versions prior to 21.4R3-S5; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; 22.4 versions prior to 22.4R2-S1, 22.4R3; 23.2 versions prior to 23.2R1-S1, 23.2R2.	2023-08 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution	

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2023-36845	Juniper	**Juniper Networks Junos OS on SRX Series and EX Series:** All versions prior to 20.4R3-S9; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S7; 21.3 versions prior to 21.3R3-S5; 21.4 versions prior to 21.4R3-S5; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; 22.4 versions prior to 22.4R2-S1, 22.4R3; 23.2 versions prior to 23.2R1-S1, 23.2R2.	2023-08 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution	
CVE-2023-36846	Juniper	**Juniper Networks Junos OS on SRX Series and EX Series:** All versions prior to 20.4R3-S9; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S7; 21.3 versions prior to 21.3R3-S5;	2023-08 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution	

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
		21.4 versions prior to 21.4R3-S5; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; 22.4 versions prior to 22.4R2-S1, 22.4R3; 23.2 versions prior to 23.2R1-S1, 23.2R2.		
CVE-2023-36847	Juniper	**Juniper Networks Junos OS on SRX Series and EX Series:** All versions prior to 20.4R3-S9; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S7; 21.3 versions prior to 21.3R3-S5; 21.4 versions prior to 21.4R3-S5; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; 22.4 versions prior to 22.4R2-S1, 22.4R3;	2023-08 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution	

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
		23.2 versions prior to 23.2R1-S1, 23.2R2.		
CVE-2023-41064	Apple	**Versions prior to:** iOS 16.6.1 and iPadOS 16.6.1, macOS Monterey 12.6.9, macOS Ventura 13.5.2, iOS 15.7.9 and iPadOS 15.7.9, macOS Big Sur 11.7.10	About the security content of iOS 16.6.1 and iPadOS 16.6.1 About the security content of macOS Ventura 13.5.2 About the security content of iOS 15.7.9 and iPadOS 15.7.9 About the security content of macOS Monterey 12.6.9 About the security content of macOS Big Sur 11.7.10	
CVE-2023-41061	Apple	**Versions prior to:** watchOS 9.6.2, iOS 16.6.1 and iPadOS 16.6.1	About the security content of watchOS 9.6.2 About the security content of iOS 16.6.1 and iPadOS 16.6.1	
CVE-2021-22205	GitLab	All versions starting from 11.9	RCE when removing metadata with ExifTool	

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2019-11510	Ivanti	Pulse Secure Pulse Connect Secure versions, 9.0R1 to 9.0R3.3, 8.3R1 to 8.3R7, and 8.2R1 to 8.2R12	SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX	
CVE-2023-6448	Unitronics	VisiLogic versions before 9.9.00	Unitronics Cybersecurity Advisory 2023-001: Default administrative password	
CVE-2017-6742	Cisco	Simple Network Management Protocol subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17	SNMP Remote Code Execution Vulnerabilities in Cisco IOS and IOS XE Software	
CVE-2021-4034	Red Hat	Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 8 Red Hat Virtualization 4 Any Red Hat product supported on Red Hat Enterprise Linux (including RHEL CoreOS) is also potentially impacted.	RHSB-2022-001 Polkit Privilege Escalation - (CVE-2021-4034)	Joint CSA: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2021-26084	Atlassian	Confluence Server and Data Center, versions 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.	Jira Atlassian: Confluence Server Webwork OGNL injection - CVE-2021-26084	Joint CSA: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure
CVE-2021-33044	Dahua	Various products	—	Joint CSA: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure
CVE-2021-33045	Dahua	Various products	—	Joint CSA: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure
CVE-2022-3236	Sophos	Sophos Firewall v19.0 MR1 (19.0.1) and older	Resolved RCE in Sophos Firewall (CVE-2022-3236)	Joint CSA: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure
CVE-2022-26134	Atlassian	Confluence Server and Data Center, versions: 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4, 7.18.1	Confluence Security Advisory 2022-06-02	Joint CSA: Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure

CVE	Vendor	Affected Products and Versions	Patch Information	Resources
CVE-2022-41040	Microsoft	Microsoft Exchange servers	Microsoft Exchange Server Elevation of Privilege Vulnerability	
CVE-2023-38831	RARLAB	WinRAR Versions prior to 6.23 Beta 1	WinRAR 6.23 Beta 1 Released	
CVE-2019-18935	Progress Telerik	Telerik.Web.UI.dll versions:	Allows JavaScriptSerializer Deserialization	Threat Actors Exploit Progress Telerik Vulnerabilities in Multiple U.S. Government IIS Servers
CVE-2021-34473	Microsoft	**Exchange Server, Multiple Versions:** Q1 2011 (2011.1.315) to R2 2017 SP1 (2017.2.621) R2 2017 SP2 (2017.2.711) to R3 2019 (2019.3.917) R3 2019 SP1 (2019.3.1023) R1 2020 (2020.1.114) and later	Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-34473	Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities