JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-215A

August 3, 2023

# 2022 Top Routinely Exploited Vulnerabilities

## SUMMARY

The following cybersecurity agencies coauthored this joint Cybersecurity Advisory (CSA):

- United States: The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI)
- 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 on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2022 and the associated Common Weakness Enumeration(s) (CWE). In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems.

---

***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 24/7 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: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.*

*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.*

The authoring agencies strongly encourage vendors, designers, developers, and end-user organizations to implement the recommendations found within the Mitigations section of this advisory—including the following—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 Secure Software Development Framework (SSDF)**, also known as SP 800-218, and implement secure design practices into each stage of the software development life cycle (SDLC). As part of this, 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, or requiring addition 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:** First check for signs of compromise if CVEs identified in this CSA have not been patched.
    - 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** and to provide links to information about how they are working to remove classes of vulnerabilities and to set secure default settings.

# TECHNICAL DETAILS

## Key Findings

In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems. Proof of concept (PoC) code was publicly available for many of the software vulnerabilities or vulnerability chains, likely facilitating exploitation by a broader range of malicious cyber actors.

Malicious cyber actors generally have the most success exploiting known vulnerabilities within the first two years of public disclosure—the value of such vulnerabilities gradually decreases as software is patched or upgraded. Timely patching reduces the effectiveness of known, exploitable vulnerabilities, possibly decreasing the pace of malicious cyber actor operations and forcing pursuit of more costly and time-consuming methods (such as developing zero-day exploits or conducting software supply chain operations).

Malicious cyber actors likely prioritize developing exploits for severe and globally prevalent CVEs. While sophisticated actors also develop tools to exploit other vulnerabilities, developing exploits for critical, wide-spread, and publicly known vulnerabilities gives actors low-cost, high-impact tools they

can use for several years. Additionally, cyber actors likely give higher priority to vulnerabilities that are more prevalent in their specific targets' networks. Multiple CVE or CVE chains require the actor to send a malicious web request to the vulnerable device, which often includes unique signatures that can be detected through deep packet inspection.

## Top Routinely Exploited Vulnerabilities

Table 1 shows the top 12 vulnerabilities the co-authors observed malicious cyber actors routinely exploiting in 2022:

- **CVE-2018-13379.** This vulnerability, affecting Fortinet SSL VPNs, was also routinely exploited in 2020 and 2021. The continued exploitation indicates that many organizations failed to patch software in a timely manner and remain vulnerable to malicious cyber actors.
- **CVE-2021-34473, CVE-2021-31207, CVE-2021-34523.** These vulnerabilities, known as ProxyShell, affect Microsoft Exchange email servers. In combination, successful exploitation enables a remote actor to execute arbitrary code. These vulnerabilities reside within the Microsoft Client Access Service (CAS), which typically runs on port 443 in Microsoft Internet Information Services (IIS) (e.g., Microsoft's web server). CAS is commonly exposed to the internet to enable users to access their email via mobile devices and web browsers.
- **CVE-2021-40539.** This vulnerability enables unauthenticated remote code execution (RCE) in Zoho ManageEngine ADSelfService Plus and was linked to the usage of an outdated third-party dependency. Initial exploitation of this vulnerability began in late 2021 and continued throughout 2022.
- **CVE-2021-26084.** This vulnerability, affecting Atlassian Confluence Server and Data Center (a web-based collaboration tool used by governments and private companies) could enable an unauthenticated cyber actor to execute arbitrary code on vulnerable systems. This vulnerability quickly became one of the most routinely exploited vulnerabilities after a PoC was released within a week of its disclosure. Attempted mass exploitation of this vulnerability was observed in September 2021.
- **CVE-2021- 44228.** This vulnerability, known as Log4Shell, affects Apache's Log4j library, an open-source logging framework incorporated into thousands of products worldwide. 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.[1] Malicious cyber actors began exploiting the vulnerability after it was publicly disclosed in December 2021, and continued to show high interest in CVE-2021- 44228 through the first half of 2022.
- **CVE-2022-22954, CVE-2022-22960.** These vulnerabilities allow RCE, privilege escalation, and authentication bypass in VMware Workspace ONE Access, Identity Manager, and other VMware products. A malicious cyber actor with network access could trigger a server-side template injection that may result in remote code execution. Exploitation of

CVE-2022-22954 and CVE-2022-22960 began in early 2022 and attempts continued throughout the remainder of the year.

- **CVE-2022-1388.** This vulnerability allows unauthenticated malicious cyber actors to bypass iControl REST authentication on F5 BIG-IP application delivery and security software.
- **CVE-2022-30190.** This vulnerability impacts the Microsoft Support Diagnostic Tool (MSDT) in Windows. A remote, unauthenticated cyber actor could exploit this vulnerability to take control of an affected system.
- **CVE-2022-26134**. This critical RCE vulnerability affects Atlassian Confluence and Data Center. The vulnerability, which was likely initially exploited as a zero-day before public disclosure in June 2022, is related to an older Confluence vulnerability (CVE-2021-26084), which cyber actors also exploited in 2022.

*Table 1: Top 12 Routinely Exploited Vulnerabilities in 2022*

| CVE | Vendor | Product | Type | CWE |
|---|---|---|---|---|
| CVE-2018-13379 | Fortinet | FortiOS and FortiProxy | SSL VPN credential exposure | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2021-34473 (Proxy Shell) | Microsoft | Exchange Server | RCE | CWE-918 Server-Side Request Forgery (SSRF) |
| CVE-2021-31207 (Proxy Shell) | Microsoft | Exchange Server | Security Feature Bypass | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2021-34523 (Proxy Shell) | Microsoft | Exchange Server | Elevation of Privilege | CWE-287 Improper Authentication |
| CVE-2021-40539 | Zoho ManageEngine | ADSelfService Plus | RCE/ Authentication Bypass | CWE-287 Improper Authentication |
| CVE-2021-26084 | Atlassian | Confluence Server and Data Center | Arbitrary code execution | CWE-74 Improper Neutralization of |

| | | | | |
|---|---|---|---|---|
| | | | | Special Elements in Output Used by a Downstream Component ('Injection') |
| CVE-2021-44228 (Log4Shell) | Apache | Log4j2 | RCE | CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')<br><br>CWE-20 Improper Input Validation<br><br>CWE-400 Uncontrolled Resource Consumption<br><br>CWE-502 Deserialization of Untrusted Data |
| CVE-2022-22954 | VMware | Workspace ONE Access and Identity Manager | RCE | CWE-94 Improper Control of Generation of Code ('Code Injection') |
| CVE-2022-22960 | VMware | Workspace ONE Access, Identity Manager, and vRealize Automation | Improper Privilege Management | CWE-269 Improper Privilege Management |
| CVE-2022-1388 | F5 Networks | BIG-IP | Missing Authentication Vulnerability | CWE-306 Missing Authentication for Critical Function |

| | | | | |
|---|---|---|---|---|
| CVE-2022-30190 | Microsoft | Multiple Products | RCE | None Listed |
| CVE-2022-26134 | Atlassian | Confluence Server and Data Center | RCE | CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') |

## Additional Routinely Exploited Vulnerabilities

In addition to the 12 vulnerabilities listed in Table 1, the authoring agencies identified vulnerabilities—listed in Table 2—that were also routinely exploited by malicious cyber actors in 2022.

*Table 2: Additional Routinely Exploited Vulnerabilities in 2022*

| CVE | Vendor | Product | Type | CWE |
|---|---|---|---|---|
| CVE-2017-0199 | Microsoft | Multiple Products | Arbitrary Code Execution | None Listed |
| CVE-2017-11882 | Microsoft | Exchange Server | Arbitrary Code Execution | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |
| CVE-2019-11510 | Ivanti | Pulse Secure Pulse Connect Secure | Arbitrary File Reading | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2019-0708 | Microsoft | Remote Desktop Services | RCE | CWE-416: Use After Free |
| CVE-2019-19781 | Citrix | Application Delivery Controller and Gateway | Arbitrary Code Execution | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2020-5902 | F5 Networks | BIG-IP | RCE | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2020-1472 | Microsoft | Multiple Products | Privilege Escalation | CWE-330: Use of Insufficiently Random Values |

| CVE | Vendor | Product | Type | CWE |
|---|---|---|---|---|
| CVE-2020-14882 | Oracle | WebLogic Server | RCE | None Listed |
| CVE-2020-14883 | Oracle | WebLogic Server | RCE | None Listed |
| CVE-2021-20016 | SonicWALL | SSLVPN SMA100 | SQL Injection | CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| CVE-2021-26855 (ProxyLogon) | Microsoft | Exchange Server | RCE | CWE-918: Server-Side Request Forgery (SSRF) |
| CVE-2021-27065 (ProxyLogon) | Microsoft | Exchange Server | RCE | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2021-26858 (ProxyLogon) | Microsoft | Exchange Server | RCE | None Listed |
| CVE-2021-26857 (ProxyLogon) | Microsoft | Exchange Server | RCE | CWE-502: Deserialization of Untrusted Data |
| CVE-2021-20021 | SonicWALL | Email Security | Privilege Escalation Exploit Chain | CWE-269: Improper Privilege Management |
| CVE-2021-40438 | Apache | HTTP Server | Server-Side Request Forgery | CWE-918: Server-Side Request Forgery (SSRF) |
| CVE-2021-41773 | Apache | HTTP Server | Server Path Traversal | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2021-42013 | Apache | HTTP Server | Server Path Traversal | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CVE-2021-20038 | SonicWall | SMA 100 Series Appliances | Stack-based Buffer Overflow | CWE-787: Out-of-bounds Write<br><br>CWE-121: Stack-based Buffer Overflow |
| CVE-2021-45046 | Apache | Log4j | RCE | CWE-917: Improper Neutralization of Special Elements used in an Expression Language |

| CVE | Vendor | Product | Type | CWE |
|---|---|---|---|---|
| | | | | Statement ('Expression Language Injection') |
| CVE-2022-42475 | Fortinet | FortiOS | Heap-based Buffer Overflow | CWE-787: Out-of-bounds Write |
| CVE-2022-24682 | Zimbra | Collaboration Suite | 'Cross-site Scripting' | CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CVE-2022-22536 | SAP | Internet Communication Manager (ICM) | HTTP Request Smuggling | CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') |
| CVE-2022-22963 | VMware Tanzu | Spring Cloud | RCE | CWE-94: Improper Control of Generation of Code ('Code Injection')<br><br>CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') |
| CVE-2022-29464 | WSO2 | Multiple Products | RCE | CWE-434: Unrestricted Upload of File with Dangerous Type |
| CVE-2022-27924 | Zimbra | Zimbra Collaboration Suite | Command Injection | CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') |
| CVE-2022-22047 | Microsoft | Windows CSRSS | Elevation of Privilege | CWE-269: Improper Privilege Management |
| CVE-2022-27593 | QNAP | QNAP NAS | Externally Controlled Reference | CWE-610: Externally Controlled Reference to a Resource in Another Sphere |
| CVE-2022-41082 | Microsoft | Exchange Server | Privilege Escalation | None Listed |
| CVE-2022-40684 | Fortinet | FortiOS, FortiProxy, FortiSwitchManager | Authentication Bypass | CWE-306: Missing Authentication for Critical Function |

# MITIGATIONS

## Vendors and Developers

The authoring agencies recommend vendors and developers take the following steps to 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 to understand which classes of vulnerability are identified more than others. Implement appropriate mitigations to eliminate those classes of vulnerability. For example, 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 that proactive steps to eliminate entire classes of security vulnerabilities, rather than only making one-off patches when new vulnerabilities are discovered.
- **Follow the SSDF** (SP 800-218) and implement secure design practices into each stage of the SDLC. Pay attention to:
    - Prioritizing the use of memory safe languages wherever possible [SSDF PW 6.1].
    - Exercising 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].
    - Setting up secure 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].
    - Establishing 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]. As part of this, establish processes to determine root causes of discovered vulnerabilities.
    - Using 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].
    - Configuring production-ready products to have to most secure settings as default and providing 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 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 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 cybersecurity posture on the basis of the 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 Cross-Sector Cybersecurity Performance Goals 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 known exploited vulnerabilities, especially those CVEs identified in this CSA, 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 CSA, refer to the appendix.
  - If a patch for a known exploited 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, and chat and other employee collaboration tools—for their customers. However, 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 Managed Service Provider Customers
    - CISA Insights Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses
    - ACSC advice on How to Manage Your Security When Engaging a Managed Service Provider
- **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 privileged accounts** (annually at a minimum) [CPG 2.D, 2.E].
- **Configure access control under the principle of least privilege** [CPG 2.Q].
    - 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 Multi-Factor Authentication 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, 2X].
    - 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 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 scanner, 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].
    - Use a network protocol analyzer to examine captured data, including packet-level data.

### *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** and to 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 through 2019, 2020, and 2021, see:
    - Joint CSA Top 10 Routinely Exploited Vulnerabilities
    - Joint CSA Top Routinely Exploited Vulnerabilities
    - Joint CSA 2021 Top Routinely Exploited Vulnerabilities
- See the appendix for additional partner resources on the vulnerabilities mentioned in this CSA.
- See ACSC's Essential Eight mitigation strategies for additional mitigations.
- See ACSC's Cyber Supply Chain Risk Management for additional considerations and advice.

## 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.

## PURPOSE

This document was developed by CISA, NSA, FBI, ACSC, CCCS, NCSC-NZ, CERT NZ, and NCSC-UK in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

## REFERENCES

[1] Apache Log4j Vulnerability Guidance

## VERSION HISTORY

August 3, 2023: Initial version.

## APPENDIX: PATCH INFORMATION AND ADDITIONAL RESOURCES FOR TOP EXPLOITED VULNERABILITIES

| CVE | Vendor | Affected Products and Versions | Patch Information | Resources |
|---|---|---|---|---|
| CVE-2017-0199 | Microsoft | Multiple Products | Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows | |
| CVE-2017-11882 | Microsoft | Office, Multiple Versions | Microsoft Office Memory Corruption Vulnerability, CVE-2017-11882 | |
| 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 | Joint CSAs:<br>Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities<br><br>Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology |

| | | | | |
|---|---|---|---|---|
| | | | | APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations |
| 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 | CISA Alerts:<br>Continued Exploitation of Pulse Secure VPN Vulnerability<br><br>Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity<br><br>ACSC Advisory:<br>2019-129: Recommendations to mitigate vulnerability in Pulse Connect Secure VPN Software<br><br>Joint CSA:<br>APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations<br><br>CCCS Alert:<br>APT Actors Target U.S. and Allied Networks - Update 1 |

| | | | | |
|---|---|---|---|---|
| CVE-2019-0708 | Microsoft | Remote Desktop Services | Remote Desktop Services Remote Code Execution Vulnerability | |
| CVE-2019-19781 | Citrix | ADC and Gateway version 13.0 all supported builds before 13.0.47.24<br><br>NetScaler ADC and NetScaler Gateway, version 12.1 all supported builds before 12.1.55.18; version 12.0 all supported builds before 12.0.63.13; version 11.1 all supported builds before 11.1.63.15; version 10.5 all supported builds before 10.5.70.12<br><br>SD-WAN WANOP appliance models 4000-WO, 4100-WO, 5000-WO, and 5100-WO all supported software release builds before 10.2.6b and 11.0.3b | CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance | Joint CSAs:<br>APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations<br><br>Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity<br><br>CCCS Alert:<br>Detecting Compromises relating to Citrix CVE-2019-19781 |

| | | | | |
|---|---|---|---|---|
| CVE-2020-5902 | F5 | BIG IP versions 15.1.0, 15.0.0 to 15.0.1, 14.1.0 to 14.1.2, 13.1.0 to 13.1.3, 12.1.0 to 12.1.5, and 11.6.1 to 11.6.5 | K52145254: TMUI RCE vulnerability CVE-2020-5902 | CISA Alert: Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902 |
| CVE-2020-1472 | Microsoft | Windows Server, Multiple Versions | Microsoft Security Update Guide: Netlogon Elevation of Privilege Vulnerability, CVE-2020-1472 | ACSC Advisory: 2020-016: Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472)<br><br>Joint CSA: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations<br><br>CCCS Alert: Microsoft Netlogon Elevation of Privilege Vulnerability - CVE-2020-1472 - Update 1 |
| CVE-2020-14882 | Oracle | WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 | Oracle Critical Patch Update Advisory - October 2020 | |

| | | | | |
|---|---|---|---|---|
| CVE-2020-14883 | Oracle | WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 | Oracle Critical Patch Update Advisory - October 2020 | |
| CVE-2021-20016 | SonicWALL | SSLVPN SMA100, Build Version 10.x | Confirmed Zero-day vulnerability in the SonicWall SMA100 build version 10.x | |
| CVE-2021-26855 | Microsoft | Exchange Server, Multiple Versions | Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26855 | CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities |
| CVE-2021-26857 | Microsoft | Exchange Server, Multiple Versions | Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26857 | CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities |
| CVE-2021-26858 | Microsoft | Exchange Server, Multiple Versions | Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26858 | CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities |
| CVE-2021-27065 | Microsoft | Multiple Products | Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-27065 | CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities |

| | | | | |
|---|---|---|---|---|
| CVE-2021-20021 | SonicWALL | Email Security version 10.0.9.x Email Security | SonicWall Email Security pre-authentication administrative account creation vulnerability | |
| CVE-2021-31207 | Microsoft | Exchange Server, Multiple Versions | Microsoft Exchange Server Security Feature Bypass Vulnerability, CVE-2021-31207 | CISA Alert: Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities<br><br>ACSC Alert: Microsoft Exchange ProxyShell Targeting in Australia |
| 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 | CISA Alert: CISA Adds One Known Exploited Vulnerability (CVE-2022-26134) to Catalog<br><br>ACSC Alert: Remote code execution vulnerability present in Atlassian Confluence Server and Data Center |
| CVE-2021-34473 | Microsoft | Exchange Server, Multiple Version | Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-34473 | Joint CSA: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities |
| CVE-2021-34523 | Microsoft | Microsoft Exchange Server 2013 Cumulative Update 23 | Microsoft Exchange Server Elevation of Privilege | CISA Alert: |

| | | | | |
|---|---|---|---|---|
| | | Microsoft Exchange Server 2016 Cumulative Updates 19 and 20<br><br>Microsoft Exchange Server 2019 Cumulative Updates 8 and 9 | Vulnerability, CVE-2021-34523 | Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities |
| CVE-2021-26084 | Jira 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 | CISA Alert: Atlassian Releases Security Updates for Confluence Server and Data Center |
| CVE-2021-40539 | Zoho ManageEngineCorp. | 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-2021-40438 | Apache | HTTP Server 2.4.48 | | |
| CVE-2021-41773 | Apache | Apache HTTP Server 2.4.49 | Apache HTTP Server 2.4 vulnerabilities | |
| CVE-2021-42013 | Apache | Apache HTTP Server 2.4.50 | Apache HTTP Server 2.4 vulnerabilities | |
| CVE-2021-20038 | SonicWall | SMA 100 Series (SMA 200, 210, 400, 410, 500v), versions 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24svSMA 100 series appliances | SonicWall patches multiple SMA100 affected vulnerabilities | ACSC Alert: Remote code execution vulnerability present in SonicWall SMA 100 series appliances |

| | | | | |
|---|---|---|---|---|
| | | | | CCCS Alert: SonicWall Security Advisory |
| CVE-2021-44228 | 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<br><br>For additional information, see joint CSA: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities | CISA webpage: Apache Log4j Vulnerability Guidance<br><br>CCCS Alert: Active exploitation of Apache Log4j vulnerability - Update 7<br><br>ACSC Advisory: 2021-007: Log4j vulnerability – advice and mitigations<br><br>ACSC Publication: Log4j: What Boards and Directors Need to Know |
| CVE-2021-45046 | Apache | Log4j 2.15.0Log4j | Apache Log4j Security Vulnerabilities | |
| CVE-2022-42475 | Fortinet | FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier and<br><br>FortiProxy SSL-VPN 7.2.0 through 7.2.1, 7.0.7 and earlier | FortiOS - heap-based buffer overflow in sslvpnd | |
| CVE-2022-24682 | Zimbra | Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1) Collaboration Suite | Zimbra Collaboration Joule 8.8.15 Patch 30 GA Release | |

| | | | | |
|---|---|---|---|---|
| CVE-2022-22536 | SAP | NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53, and SAP Web Dispatcher Internet Communication Manager (ICM) | Remediation of CVE-2022-22536 Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher | CISA Alert: Critical Vulnerabilities Affecting SAP Applications Employing Internet Communication Manager (ICM) |
| CVE-2022-22963 | VMware Tanzumware Tanzu | Spring Cloud Function versions 3.1.6, 3.2.2, and older unsupported versions | CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression | |
| CVE-2022-22954 | VMware | Workspace ONE Access, versions 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0<br><br>Identity Manager (vIDM) 3.3.6, 3.3.5, 3.3.4, 3.3.3<br>vRealize Automation (vIDM), 8.x, 7.6<br>VMware Cloud Foundation (vIDM), 4.x<br><br>vRealize Suite Lifecycle Manager (vIDM), 8.xWorkspace | VMware Advisory VMSA-2022-0011 | |

| | | | | |
|---|---|---|---|---|
| | | ONE Access and Identity Manager | | |
| CVE-2022-22960 | VMware | Workspace ONE Access, versions 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0<br>Identity Manager (vIDM) and vRealize Automation3.3.6, 3.3.5, 3.3.4, 3.3.3<br><br>vRealize Automation (vIDM), 8.x, 7.6<br><br>VMware Cloud Foundation (vIDM), 4.x<br><br>VMware Cloud Foundation (vRA), 3.x<br><br>vRealize Suite Lifecycle Manager (vIDM), 8.x | VMSA-2022-0011 | |

| | | | | |
|---|---|---|---|---|
| CVE-2022-29464 | AtlassianWSO2 | WSO2 API Manager 2.2.0 and above through 4.0.0<br><br>WSO2 Identity Server 5.2.0 and above through 5.11.0<br><br>WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0<br><br>WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0<br><br>WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0 | WSO2 Documentation - Spaces | |
| CVE-2022-27924 | Zimbra | Zimbra Collaboration Suite, 8.8.15 and 9.0 | Zimbra Collaboration Kepler 9.0.0 Patch 24.1 GA Release | |
| CVE-2022-1388 | F5 Networks | F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and All 12.1.x and 11.6.x versions | K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388 | Joint CSA: Threat Actors Exploiting F5 BIG-IP CVE-2022-1388 |

| | | | | |
|---|---|---|---|---|
| CVE-2022-30190 | Microsoft | Exchange Server, Multiple Versions | | CISA Alert: Microsoft Releases Workaround Guidance for MSDT "Follina" Vulnerability |
| CVE-2022-22047 | Microsoft | Multiple Products | Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability, CVE-2022-22047 | |
| CVE-2022-27593 | QNAP | Certain QNAP NAS running Photo Station with internet exposure Ausustor Network Attached Storage | DeadBolt Ransomware | |

| | | | | |
|---|---|---|---|---|
| CVE-2022-41082 | Microsoft | Exchange Server 2016 Cumulative Update 23, 2019 Cumulative Update 12, 2019 Cumulative Update 11, 2016 Cumulative Update 22, and 2013 Cumulative Update 23 | Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2022-41082 | ACSC Alert: Vulnerability Alert – 2 new Vulnerabilities associated with Microsoft Exchange. |
| CVE-2022-40684 | Fortinet | FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 | FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface | |