



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

CYBERSECURITY ADVISORY

2021 Top Routinely Exploited Vulnerabilities

Last Revised: April 28, 2022

Alert Code: AA22-117A



Summary

This joint Cybersecurity Advisory (CSA) was coauthored by cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom: the Cybersecurity and Infrastructure Security Agency ([CISA](https://www.cisa.gov/)), National Security Agency ([NSA](https://www.nsa.gov/cybersecurity/)), Federal Bureau of Investigation ([FBI](https://www.fbi.gov/investigate/cyber)), Australian Cyber Security Centre ([ACSC](https://www.cyber.gov.au/)), Canadian Centre for Cyber Security ([CCCS](https://www.cyber.gc.ca/en/)), New Zealand National Cyber Security Centre ([NZ NCSC](https://www.gcsb.govt.nz/)), and United Kingdom's National Cyber Security Centre ([NCSC-UK](https://www.ncsc.uk.gov/)).

[Give Feedback](#)

<<https://www.ncsc.gov.uk/>>). This advisory provides details on the top 15 Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors in 2021, as well as other CVEs frequently exploited.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities assess, in 2021, malicious cyber actors aggressively targeted newly disclosed critical software vulnerabilities against broad target sets, including public and private sector organizations worldwide. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities across a broad spectrum of targets.

The cybersecurity authorities encourage organizations to apply the recommendations in the Mitigations section of this CSA. These mitigations include applying timely patches to systems and implementing a centralized patch management system to reduce the risk of compromise by malicious cyber actors.

Download the [Joint Cybersecurity Advisory: 2021 top Routinely Exploited Vulnerabilities \(pdf, 777kb\)](#). <[/sites/default/files/publications/aa22-117a_joint_csa_2021_top_routinely_exploited_vulnerabilities_final.pdf](https://sites/default/files/publications/aa22-117a_joint_csa_2021_top_routinely_exploited_vulnerabilities_final.pdf)>

Technical Details

Key Findings

Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities. For most of the top exploited vulnerabilities, researchers or other actors released proof of concept (POC) code within two weeks of the vulnerability's disclosure, likely facilitating exploitation by a broader range of malicious actors.

To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities—some of which were also [routinely exploited in 2020](#) <<https://www.cisa.gov/uscert/ncas/alerts/aa21-209a>> or earlier. The exploitation of older

Give Feedback

vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.

Top 15 Routinely Exploited Vulnerabilities

Table 1 shows the top 15 vulnerabilities U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities observed malicious actors routinely exploiting in 2021, which include:

- **CVE-2021-44228.** This vulnerability, known as Log4Shell, affects Apache's Log4j library, an open-source logging framework. An actor can exploit this vulnerability by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows a cyber actor to take full control over the system. The actor can then steal information, launch ransomware, or conduct other malicious activity.[1] Log4j is incorporated into thousands of products worldwide. This vulnerability was disclosed in December 2021; the rapid widespread exploitation of this vulnerability demonstrates the ability of malicious actors to quickly weaponize known vulnerabilities and target organizations before they patch.
- **CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065.** These vulnerabilities, known as ProxyLogon, affect Microsoft Exchange email servers. Successful exploitation of these vulnerabilities in combination (i.e., “vulnerability chaining”) allows an unauthenticated cyber actor to execute arbitrary code on vulnerable Exchange Servers, which, in turn, enables the actor to gain persistent access to files and mailboxes on the servers, as well as to credentials stored on the servers. Successful exploitation may additionally enable the cyber actor to compromise trust and identity in a vulnerable network.
- **CVE-2021-34523, CVE-2021-34473, CVE-2021-31207.** These vulnerabilities, known as ProxyShell, also affect Microsoft Exchange email servers. Successful exploitation of these vulnerabilities in combination 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.

Give Feedback

- **CVE-2021-26084.** This vulnerability, affecting Atlassian Confluence Server and Data Center, could enable an unauthenticated 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.

Three of the top 15 routinely exploited vulnerabilities were also [routinely exploited in 2020](https://www.cisa.gov/uscert/ncas/alerts/aa21-209a) <<https://www.cisa.gov/uscert/ncas/alerts/aa21-209a>>: CVE-2020-1472, CVE-2018-13379, and CVE-2019-11510. Their continued exploitation indicates that many organizations fail to patch software in a timely manner and remain vulnerable to malicious cyber actors.

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228 < https://nvd.nist.gov/vuln/detail/cve-2021-44228 >	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539 < https://nvd.nist.gov/vuln/detail/cve-2021-40539 >	Zoho ManageEngine AD SelfService Plus	Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523 < https://nvd.nist.gov/vuln/detail/cve-2021-34523 >	ProxyShell	Microsoft Exchange Server	Elevation of privilege

Give Feedback

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-34473 < https://nvd.nist.gov/vuln/detail/cve-2021-34473 >	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207 < https://nvd.nist.gov/vuln/detail/cve-2021-31207 >	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065 < https://nvd.nist.gov/vuln/detail/cve-2021-27065 >	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858 < https://nvd.nist.gov/vuln/detail/cve-2021-26858 >	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857 < https://nvd.nist.gov/vuln/detail/cve-2021-26857 >	ProxyLogon	Microsoft Exchange Server	RCE

Give Feedback

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-26855 < https://nvd.nist.gov/vuln/detail/cve-2021-26855 >	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084 < https://nvd.nist.gov/vuln/detail/cve-2021-26084 >		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972 < https://nvd.nist.gov/vuln/detail/cve-2021-21972 >		VMware vSphere Client	RCE
CVE-2020-1472 < https://nvd.nist.gov/vuln/detail/cve-2020-1472 >	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688 < https://nvd.nist.gov/vuln/detail/cve-2020-0688 >		Microsoft Exchange Server	RCE

Give Feedback

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2019-11510 < https://nvd.nist.gov/vuln/detail/cve-2019-11510 >		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379 < https://nvd.nist.gov/vuln/detail/cve-2018-13379 >		Fortinet FortiOS and FortiProxy	Path traversal

Additional Routinely Exploited Vulnerabilities

In addition to the 15 vulnerabilities listed in table 1, U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities identified vulnerabilities, listed in table 2, that were also routinely exploited by malicious cyber actors in 2021.

These vulnerabilities include multiple vulnerabilities affecting internet-facing systems, including Accellion File Transfer Appliance (FTA), Windows Print Spooler, and Pulse Secure Pulse Connect Secure. Three of these vulnerabilities were also [routinely exploited in 2020](#) <<https://www.cisa.gov/uscert/ncas/alerts/aa21-209a>>: CVE-2019-19781, CVE-2019-18935, and CVE-2017-11882.

Give Feedback

Table 2: Additional Routinely Exploited Vulnerabilities in 2021

CVE	Vendor and Product	Type
CVE-2021-42237 < https://nvd.nist.gov/vuln/detail/cve-2021-42237 >	Sitecore XP	RCE

CVE	Vendor and Product	Type
CVE-2021-35464 < https://nvd.nist.gov/vuln/detail/cve-2021-35464 >	ForgeRock OpenAM server	RCE
CVE-2021-27104 < https://nvd.nist.gov/vuln/detail/cve-2021-27104 >	Accellion FTA	OS command execution
CVE-2021-27103 < https://nvd.nist.gov/vuln/detail/cve-2021-27103 >	Accellion FTA	Server-side request forgery
CVE-2021-27102 < https://nvd.nist.gov/vuln/detail/cve-2021-27102 >	Accellion FTA	OS command execution
CVE-2021-27101 < https://nvd.nist.gov/vuln/detail/cve-2021-27101 >	Accellion FTA	SQL injection
CVE-2021-21985 < https://nvd.nist.gov/vuln/detail/cve-2021-21985 >	VMware vCenter Server	RCE
CVE-2021-20038 < https://nvd.nist.gov/vuln/detail/cve-2021-20038 >	SonicWall Secure Mobile Access (SMA)	RCE
CVE-2021-40444 < https://nvd.nist.gov/vuln/detail/cve-2021-40444 >	Microsoft MSHTML	RCE

Give Feedback

CVE	Vendor and Product	Type
CVE-2021-34527 < https://nvd.nist.gov/vuln/detail/cve-2021-34527 >	Microsoft Windows Print Spooler	RCE
CVE-2021-3156 < https://nvd.nist.gov/vuln/detail/cve-2021-3156 >	Sudo	Privilege escalation
CVE-2021-27852 < https://nvd.nist.gov/vuln/detail/cve-2021-27852 >	Checkbox Survey	Remote arbitrary code execution
CVE-2021-22893 < https://nvd.nist.gov/vuln/detail/cve-2021-22893 >	Pulse Secure Pulse Connect Secure	Remote arbitrary code execution
CVE-2021-20016 < https://nvd.nist.gov/vuln/detail/cve-2021-20016 >	SonicWall SSLVPN SMA100	Improper SQL command neutralization, allowing for credential access
CVE-2021-1675 < https://nvd.nist.gov/vuln/detail/cve-2021-1675 >	Windows Print Spooler	RCE
CVE-2020-2509 < https://nvd.nist.gov/vuln/detail/cve-2020-2509 >	QNAP QTS and QuTS hero	Remote arbitrary code execution
CVE-2019-19781 < https://nvd.nist.gov/vuln/detail/cve-2019-19781 >	Citrix Application Delivery Controller (ADC) and Gateway	Arbitrary code execution

Give Feedback

CVE	Vendor and Product	Type
CVE-2019-18935 < https://nvd.nist.gov/vuln/detail/cve-2019-18935 >	Progress Telerik UI for ASP.NET AJAX	Code execution
CVE-2018-0171 < https://nvd.nist.gov/vuln/detail/cve-2018-0171 >	Cisco IOS Software and IOS XE Software	Remote arbitrary code execution
CVE-2017-11882 < https://nvd.nist.gov/vuln/detail/cve-2017-11882 >	Microsoft Office	RCE
CVE-2017-0199 < https://nvd.nist.gov/vuln/detail/cve-2017-0199 >	Microsoft Office	RCE

Mitigations

Vulnerability and Configuration Management

- Update software, operating systems, applications, and firmware on IT network assets a timely manner. Prioritize patching [known exploited vulnerabilities](#) <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>>, especially those CVEs identified in this CSA, and 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.
- Use a centralized patch management system.
- Replace end-of-life software, i.e., software that is no longer supported by the vendor. For example, Accellion FTA was retired in April 2021.

Give Feedback

- 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, as MSPs and CSPs expand their client organization's attack surface and may introduce unanticipated risks, organizations should proactively collaborate with their MSPs and CSPs to jointly reduce that risk. For more information and guidance, see the following resources.
 - CISA Insights [Risk Considerations for Managed Service Provider Customers](https://cisa.gov/sites/default/files/publications/cisa-insights_risk-considerations-for-msp-customers_508.pdf) <https://cisa.gov/sites/default/files/publications/cisa-insights_risk-considerations-for-msp-customers_508.pdf>
 - CISA Insights [Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses](https://cisa.gov/sites/default/files/publications/cisa%20insights_guidance-for-msps-and-small-and-mid-sized-businesses_s508c.pdf) <https://cisa.gov/sites/default/files/publications/cisa%20insights_guidance-for-msps-and-small-and-mid-sized-businesses_s508c.pdf>
 - ACSC advice on [How to Manage Your Security When Engaging a Managed Service Provider](#)

Identity and Access Management

- Enforce multifactor authentication (MFA) for all users, without exception.
- Enforce MFA on all VPN connections. If MFA is unavailable, require employees engaging in remote work to use strong passwords.
- Regularly review, validate, or remove privileged accounts (annually at a minimum).
- Configure access control under the concept of least privilege principle.
 - Ensure software service accounts only provide necessary permissions (least privilege) to perform intended functions (non-administrative privileges).

Give Feedback

Note: see [CISA Capacity Enhancement Guide – Implementing Strong Authentication](https://cisa.gov/sites/default/files/publications/cisa_ceg_implementing_strong_authentication_508_1.pdf)

<https://cisa.gov/sites/default/files/publications/cisa_ceg_implementing_strong_authentication_508_1.pdf>

and ACSC guidance on [Implementing Multi-Factor Authentication](#) for more information on hardening authentication systems.

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.
 - 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).
- Segment networks to limit or block lateral movement by controlling access to applications, devices, and databases. Use private virtual local area networks.
- Continuously monitor the attack surface and investigate abnormal activity that may indicate lateral movement of a threat actor or malware.
 - 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 your EDR, SIEM, vulnerability scanner etc., are reporting the same number of assets.
 - Monitor the environment for potentially unwanted programs.
- Reduce third-party applications and unique system/application builds; provide exceptions only if required to support business critical functions.
- Implement application allowlisting.

Resources

- For the top vulnerabilities exploited in 2020, see joint CSA [Top Routinely Exploited Vulnerabilities](https://www.cisa.gov/uscert/ncas/alerts/aa21-209a) <<https://www.cisa.gov/uscert/ncas/alerts/aa21-209a>>
- For the top exploited vulnerabilities 2016 through 2019, see joint CSA [Top 10 Routinely Exploited Vulnerabilities](https://www.cisa.gov/uscert/ncas/alerts/aa20-133a) <<https://www.cisa.gov/uscert/ncas/alerts/aa20-133a>>.

Give Feedback

- See the appendix for additional partner resources on the vulnerabilities mentioned in this CSA.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. CISA, the FBI, NSA, ACSC, CCCS, NZ NCSC, 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 U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

References

[1] CISA’s Apache Log4j Vulnerability Guidance <<https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>>

Appendix: Patch Information and Additional Resources for Top Exploited Vulnerabilities

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-42237 < https://nvd.nist.gov/vuln/detail/cve-2021-42237 >	Sitecore	Sitecore XP 7.5.0 - Sitecore XP 7.5.2 Sitecore XP 8.0.0 - Sitecore XP 8.2.7	Sitecore Security Bulletin SC2021-003-499266	ACSC Alert Active Exploitaton of vulnerable Sitecore Experience Platform Content Management Systems < https://www.cyber.gov.au/about-us/alerts/active-exploitation-vulnerable-sitecore-experience-platform-content

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			management systems>	

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-35464<https://nvd.nist.gov/vuln/detail/cve-2021-35464>	ForgeRock	Access Management (AM) 5.x, 6.0.0.x, 6.5.0.x, 6.5.1, 6.5.2.x and 6.5.3 OpenAM 9.x, 10.x, 11.x, 12.x and 13.x	ForgeRock AM Security Advisory #202104 <https://backstage.forgerock.com/knowledge/kb/article/a47894244>	ACSC Advisory Active exploitati on of ForgeRock Access Manager / OpenAM servers <https://www.cyber.gov.au/about - us/advisories/advisory-2021-004-active-exploitatio n-forgerock-access-manager-openam-servers> CCCS ForgeRock Security

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
				Advisory < https://w ww.cyber.g c.ca/en/ale rts/forgero ck- security- advisory>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-27104 < https://nvd.nist.gov/vuln/detail/cve-2021-27104 >	Accellion	FTA 9_12_370 and earlier	Accellion Press Release: Update to Recent FTA Security Incident < https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ >	Joint CSA Exploitation of Accellion File Transfer Appliance < https://www.cisa.gov/uscert/ncas/alerts/a21-055a > ACSC Alert Potential Accellion File Transfer Appliance
CVE-2021-27103 < https://nvd.nist.gov/vuln/detail/cve-2021-27103 >		FTA 9_12_411 and earlier		
CVE-2021-27102 < https://nvd.nist.gov/vuln/detail/cve-2021-27102 >		FTA versions 9_12_411 and earlier		< https://www.cyber.gov.au/about-us/alerts/potential-accellion- >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-27101 < https://nvd.nist.gov/vuln/detail/cve-2021-27101 >		FTA 9_12_370 and earlier		file-transfer-appliance-compromise>
CVE-2021-21985 < https://nvd.nist.gov/vuln/detail/cve-2021-21985 >	VMware	vCenter Server 7.0, 6.7, 6.5 Cloud Foundation (vCenter Server) 4.x and 3.x	VMware Advisory VMSA-2021-0010 < https://www.vmware.com/security/advisories/vmsa-2021-0010.html >	CCCS VMware Security Advisory < https://www.cyber.gc.ca/en/alerts/mts/vmware-security-advisory-41 >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-21972 <https://nvd.nist.gov/vuln/detail/cve-2021-21972>	VMware	vCenter Server 7.0, 6.7, 6.5 Cloud Foundation (vCenter Server) 4.x and 3.x	VMware Advisory VMSA-2021-0002 <https://www.vmware.com/security/advisories/vmsa-2021-0002.html>	ACSC Alert VMware vCenter Server plugin remote code execution vulnerability <https://www.cyber.gov.au/about-us/alerts/vmware-vcenter-server-plugin-remote-code-execution-vulnerability-cve-2021-21972> <div style="background-color: #0056b3; color: white; padding: 5px; text-align: right;">Give Feedback</div>

CVE	Vendor	Affected Products	Patch Information	Resources
				CCCS VMware Security Advisory <https://w ww.cyber.g c.ca/en/ale rts/vmware -security- advisory- 35>
				CCCS Alert APT Actors Target U.S. and Allied Networks -Update 1 <https://w ww.cyber.g c.ca/en/ale rts/apt- actors- target-us- and-allied- networks- nsacisafbi>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-20038 <https://nvd.nist.gov/vuln/detail/cve-2021-20038>	SonicWall	SMA 100 Series (SMA 200, 210, 400, 410, 500v), versions 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv	SonicWall Security Advisory SNWLID-2021-0026 <https://psi.rt.global.ssl.fastly.net/global.sonicwall.com/vulnerability/detail/snwlid-2021-0026>	ACSC Alert Remote code execution vulnerability present in SonicWall SMA 100 series appliances <https://www.cyber.gov.au/about-us/alerts/remote-code-execution-vulnerability-present-sonicwall-sma-100-

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			series-appliances >	CCCS SonicWall Security Advisory < https://www.cyber.gc.ca/en/alerts/sonicwall-security-advisory-4 >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
<p>CVE-2021-44228 <https://nvd.nist.gov/vuln/detail/cve-2021-44228></p>	Apache	<p>Log4j, all versions from 2.0-beta9 to 2.14.1</p> <p>For other affected vendors and products, see CISA's GitHub repository</p>	<p>Log4j: Apache Log4j Security Vulnerabilities <https://logging.apache.org/log4j/2.x/security.html></p> <p>For additional information, see Joint CSA: Mitigating Log4Shell and Log4j-Related Vulnerabilities</p> <p>Other Log4j-Related Vulnerabilities <https://www.cisa.gov/uscert/apache-log4j-vulnerability-y-guidance></p>	<p>CISA webpage</p> <p>Apache Log4j Security Log4j Vulnerability Guidance <https://www.cisa.gov/uscert/apache-log4j-vulnerability-y-guidance></p> <p>CCCS Active exploitation on of Apache Log4j Vulnerability - Update 7 <https://www.cyber.gc.ca/en/alerts/active-exploitatio></p> <p><https://www.cisa.gov/uscert/apache-log4j-vulnerability-y-guidance></p>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			v/uscert/nc as/alerts/a a21-356a>	log4j- vulnerabilit y>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-40539 <https://nvd.nist.gov/vuln/detail/cve-2021-40539>	Zoho ManageEngine	ADSelfService Plus version 6113 and prior	Zoho ManageEngine: ADSelfService Plus 6114 Security Fix Release <https://pitstop.manageengine.com/portal/en/community/topic/adsselfservice-plus-6114-security-fix-release>	Joint CSA APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus <https://www.cisa.gov/uscert/ncas/alerts/aa21-259a> CCCS Zoho Security Advisory <https://www.cyber.gc.ca/en/alerts/zoho-security-advisory>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-40444 < https://nvd.nist.gov/vuln/detail/cve-2021-40444 >	Microsoft	Multiple Windows products; see Microsoft Security Update Guide: MSHTML Remote Code Execution MSHTML Remote Code Execution Vulnerability, CVE-2021-40444 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-40444 >	Microsoft Security Update Guide: MSHTML Remote Code Execution	Vulnerability, CVE-2021-40444 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-40444 >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-34527 <https://nvd.nist.gov/vuln/detail/cve-2021-34527>	Microsoft	Multiple Windows products; see Microsoft Security Update Guide: Windows Print Spooler Remote Code Execution Vulnerability, CVE-2021-34527 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-34527>	Microsoft Security Update Guide: Windows Print Spooler Remote Code Execution Vulnerability, CVE-2021-34527 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-34527>	Joint CSA Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability <https://www.cisa.gov/uscert/ncas/alerts/a22-074a> CCCS Alert Windows

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2023-3029	Microsoft	Windows Print Spooler	Print Spooler Vulnerability Remains Unpatched - Update 3 < https://www.cyber.gc.ca/en/alerts/windows/print-spooler-vulnerability-remains-unpatched/ >	Print Spooler Vulnerability Remains Unpatched - Update 3 < https://www.cyber.gc.ca/en/alerts/windows/print-spooler-vulnerability-remains-unpatched/ >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-34523 < https://nvd.nist.gov/vuln/detail/cve-2021-34523 >	Microsoft	Microsoft Exchange Server 2013 Cumulative Update 23 Microsoft Exchange Server 2016 Cumulative Updates 19 and 20 Microsoft Exchange Server 2019 Cumulative Updates 8 and 9	Microsoft Security Update Guide: Microsoft Exchange Server Elevation of Privilege Vulnerability, CVE-2021-34523 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-34523 >	Joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities

Give Feedback

ACSC Alert Microsoft Exchange

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-34473 <https://nvd.nist.gov/vuln/detail/cve-2021-34473>	Microsoft	Multiple Exchange Server versions; see: Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-34473 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-34473>	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-34473 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-34473>	ProxyShell Targeting in Australia <https://www.cyber.gov.au/about-us/alerts/microsoft-exchange-proxyshell-targeting-australia#:~:text=the%20australian%20signature%20directory%20with%20upload%20with> Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-31207 < https://nvd.nist.gov/vuln/detail/cve-2021-31207 >	Microsoft	Multiple Exchange Server versions; see Microsoft Update Guide: Microsoft Exchange Server Security Feature Bypass Vulnerability, CVE-2021-31207 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-31207 >	Microsoft Update Guide: Microsoft Exchange Server Security Feature Bypass Vulnerability, CVE-2021-31207 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-31207 >	

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-3156 < https://nvd.nist.gov/vuln/detail/cve-2021-3156 >	Sudo	Sudo before 1.9.5p2	Sudo Stable Release 1.9.5p2 < https://www.sudo.ws/releases/stable/#1.9.5p2 >	
CVE-2021-27852 < https://nvd.nist.gov/vuln/detail/cve-2021-27852 >	Checkbox Survey	Checkbox Survey versions prior to 7		

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-27065 <https://nvd.nist.gov/vuln/detail/cve-2021-27065>	Microsoft Exchange Server	Multiple versions; see: Microsoft Security Update Guide: Microsoft Exchange Server Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-27065 Vulnerability, CVE-2021-27065 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-27065> Vulnerability, CVE-2021-27065 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-27065>	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-27065 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-27065>	CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities <https://www.cisa.gov/uscert/ncas/alerts/a21-062a> ACSC Advisory Active exploitation of Vulnerable Microsoft Exchange servers <https://www.cyber.gov.au/about-us/advisories/advisory-2021-002-

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-26858 < https://nvd.nist.gov/vuln/detail/cve-2021-26858 >	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide:	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26858 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-26858 >	active-exploitatio n-vulnerable-microsoft-exchange-servers> CCCS Alert Active Exploitati on of Microsoft Exchange Vulnerabi lities - Update 4 < https://www.cyber.gc.ca/en/alerts/active-exploitatio-n-microsoft-exchange-vulnerabilitie >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-26857 <https://nvd.nist.gov/vuln/detail/cve-2021-26857>	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26857	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26857	https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-26857

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-26855 < https://nvd.nist.gov/vuln/detail/cve-2021-26855 >	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26855 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-26855 >	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution n Vulnerability, CVE-2021-26855 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-26855 >	

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-26084 < https://nvd.nist.gov/vuln/detail/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 < https://jira.atlassian.com/browse/CONFSERVER-67940 >	ACSC Alert Remote code execution vulnerability present in certain versions of Atlassian Confluence CCCS Atlassian Security Advisory < https://www.cyber.gc.ca/en/alerts/atlassian-security-advisory >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-22893 < https://nvd.nist.gov/vuln/detail/cve-2021-22893 >	Pulse Secure	PCS 9.0R3/9.1 R1 and Higher	Pulse Secure SA44784-2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4 < https://kb.pulsesecure.net/articles/pulse_security_advories/sa44784/ >	CCCS Alert Active Exploitation of Pulse Connect Secure Vulnerabilities - Update 1 < https://www.cib.ca/en/alerts/active-exploitations/pulse-connect-secure-vulnerabilities >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-20016 < https://nvd.nist.gov/vuln/detail/cve-2021-20016 >	SonicWall	SMA 100 devices (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v)	SonicWall Security Advisory SNWLID-2021-0001 < https://psi.rt.global.sonicwall.com/vulnerability-detail/snwlid-2021-0001 >	

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-1675 < https://nvd.nist.gov/vuln/detail/cve-2021-1675 >	Microsoft	Multiple Windows products; see Microsoft Security Update Guide.	Microsoft Windows Print Spooler Remote Code Execution Vulnerability, CVE-2021-1675 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2021-1675 >	CCCS Alert Windows Print Spooler Vulnerability Remains Unpatched - Update 3 < https://www.cisa.gov/cisa-en/arts/windows-print-spooler-vulnerability-remains-unpatched >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-2509 < https://nvd.nist.gov/vuln/detail/cve-2020-2509 >	QNAP	QTS, multiple versions; see QNAP: Command Injection Vulnerability in QTS and QuTS hero	QNAP: Command Injection Vulnerability in QTS and QuTS hero	QuTS hero

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-1472 < https://nvd.nist.gov/vuln/detail/cve-2020-1472 >	Microsoft	Windows Server, multiple versions; see Microsoft Security Update Guide: Netlogon Elevation of Privilege Vulnerability, CVE-2020-1472 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2020-1472 >	Microsoft Security Update Guide: Netlogon Elevation of Privilege Vulnerability, CVE-2020-1472 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2020-1472 >	ACSC Alert Netlogon elevation of privilege vulnerability (CVE-2020-1472) < https://www.cyber.gov.au/about/ -< https://us/alerts/netlogon-elevation-privilege-vulnerability-cve-2020-1472 >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-1472	Microsoft	Netlogon Elevation of Privilege Vulnerability	Update 1 https://www.cisa.gov/uscert/ncas/alerts/aa20-283a	CCCS Alert Microsoft Netlogon Elevation of Privilege Vulnerability - CVE-2020-1472 - Update 1 https://www.cyber.gc.ca/en/alerts/microsoft-netlogon-
				Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			elevation-privilege-vulnerability-cve-2020-1472>	

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-0688 <https://nvd.nist.gov/vuln/detail/cve-2020-0688>	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide: Microsoft Exchange Validation Key Remote Code Execution Vulnerability, CVE-2020-0688 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2020-0688>	Microsoft Security Update Guide: Microsoft Exchange Validation Key Remote Code Execution Vulnerability, CVE-2020-0688 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2020-0688>	CISA Alert Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity <https://www.cisa.gov/uscert/ncas/alerts/a20-258a> Joint CSA Russian State-Sponsored Cyber Actors Target Cleared Defense Contract or Networks to Obtain Sensitive

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			U.S. Defense Information and Technology https://www.cisa.gov/uscert/ncas/alerts/aa22-047a	
			CCCS Alert Microsoft Exchange Validation Key Remote Code Execution Vulnerability https://www.cyber.gc.ca/en/alerts/microsoft-exchange	Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			validation-key-remote-code-execution-vulnerability>	

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2019-19781 < https://nvd.nist.gov/vuln/detail/cve-2019-19781 >	Citrix	ADC and Gateway version 13.0 all supported builds before 13.0.47.2 NetScaler ADC and NetScaler Gateway, version 12.1 all supported builds before 12.1.55.18 ; version 12.0 all supported builds before 12.0.63.1 3; version 11.1 all supported	Citrix Security Bulletin CTX2670 27	Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations https://www.cisa.gov/uscert/ncas/alerts/aa20-283a

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
		d builds before 11.1.63.15; version 10.5 all supported d builds before 10.5.70.12 SD-WAN WANOP appliances e models 4000-WO, 4100-WO, 5000-WO, and 5100-WO all supported software release builds before 10.2.6b and 11.0.3b	< https://www.cisa.gov/uscert/ncas/alerts/a20-258a >	Activity CCCS Alert Detection Compromises relating to Citrix CVE-2019-19781 < https://www.cyber.gc.ca/en/alerts/detecting-compromises-relating-citrix-cve-2019-19781-0 >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2019-18935 <https://nvd.nist.gov/vuln/detail/cve-2019-18935>	Progress Telerik	UI for ASP.NET AJAX through 2019.3.10.23	Telerik UI for ASP.NET AJAX Allows JavaScriptSerialize or Deserialization <https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/common-allowsscript-serializer-deserialization>	ACSC Alert Active exploitati on of vulnerabi lity in Microsoft Internet Informati on Services <https://www.cyber.gov.au/about-us/advisories/advisory-2020-004-remote-code-execution-vulnerability-being-actively-exploited-vulnerable-versions-

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2024-3523	Telerik UI for ASP.NET Core	RadGrid, RadEditor, RadForm	Published on 2024-05-15 Patch available for .NET Framework 4.8 and later	View Details Report a Problem telerik-ui-sophisticated-actors>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2019-11510 < https://nvd.nist.gov/vuln/detail/cve-2019-11510 >	Pulse Secure	Pulse Connect Secure before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4	Pulse Secure: SA44101-2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX < https://kb.pulsesecure.net/articles/pulse_security_advisories/sa44101/ >	CISA Alert Continued Exploitation of Pulse Secure VPN Vulnerability https://www.cisa.gov/uscert/ncas/alerts/a20-010a CISA Alert Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity < https://www.cisa.gov >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
<p>v/uscert/nc as/alerts/a a20-258a></p> <p>ACSC Advisory Recommendations to mitigate vulnerability in Pulse Connect Secure VPN Software</p> <p>Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations</p>				Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-283a	Microsoft	Windows, Microsoft Office, Internet Explorer	https://www.cisa.gov/uscert/ncas/alerts/aa20-283a	tions <https://w ww.cisa.go v/uscert/nc as/alerts/a a20-283a>
CVE-2020-283b	Microsoft	Windows, Microsoft Office, Internet Explorer	https://www.cyber.gc.ca/en/alerts/apt-actors-target-us-and-allied-networks-target-us-and-allied-networks-nsacisafbi	CCCS Alert APT Actors Target U.S. and Allied Networks -Update 1 <https://w ww.cyber.g c.ca/en/ale rts/apt- actors- target-us- and-allied- networks- nsacisafbi>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2018-13379<https://nvd.nist.gov/vuln/detail/cve-2018-13379>	Fortinet	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	Fortinet FortiGuard Labs: FG-IR-20-233 <https://www.fortiguard.com/patch/fg-ir-20-233>	Joint CSA Russian State-Sponsored Cyber Actors Target Cleared Defense Contract or Networks to Obtain Sensitive U.S. Defense Information and Technology <https://www.cisa.gov/uscert/ncas/alerts/a22-047a>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-321a	Microsoft Exchange and Fortinet	Microsoft Exchange and Fortinet	Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities	<p>Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure</p> <p><https://www.cisa.gov/uscert/ncas/alerts/a21-321a></p>
CVE-2021-321b	Cyber Actors Exploiting Microsoft Exchange	Cyber Actors Exploiting Microsoft Exchange	Cyber Actors Exploiting Microsoft Exchange	Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-283a	Cisco	Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software	Cisco released a patch for this vulnerability. The patch is available for download from the Cisco website. It is recommended to apply the patch as soon as possible.	Picture, and Elections Organizations < https://www.cisa.gov/uscert/ncas/alerts/aa20-283a >
CVE-2020-283b	Fortinet	Fortinet FortiGate, FortiWALL, and FortiSwitch products	Fortinet released a patch for this vulnerability. The patch is available for download from the Fortinet website. It is recommended to apply the patch as soon as possible.	ACSC Alert APT exploitati on of Fortinet Vulnerabi lities < https://www.cyber.gov.au/about-us/alerts/aps-exploitatio-n-fortinet-vulnerabiliti es >

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
			CCCS Alert Exploitati on of Fortinet FortiOS vulnerabi lities (CISA, FBI) - Update 1 <https://w ww.cyber.g c.ca/en/ale rts/exploita tion- fortinet- fortios- vulnerabilit ies-cisa- fbi>	Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2018-0171<https://nvd.nist.gov/vuln/detail/cve-2018-0171>	Cisco	See Cisco Security Advisory: cisco-sa-20180328-smi2<https://tools.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-20180328-smi2#fixed>	Cisco Security Advisory: cisco-sa-20180328-smi2<https://tools.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-20180328-smi2#fixed>	CCCS Action Required to Secure the Cisco IOS and IOS XE Smart Install Feature <https://www.cyber.gc.ca/en/actions/required-secure-cisco-ios-and-ios-xe-smart-install-feature>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2017-11882 <https://nvd.nist.gov/vuln/detail/cve-2017-11882>	Microsoft	Office, multiple versions; see Microsoft Security Update Guide: Microsoft Security Office Update Memory Corruption Guide: Microsoft Office Memory Corruption Vulnerability, CVE-2017-11882 Vulnerability, CVE-2017-11882 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2017-11882>	Microsoft Security Update Guide: Microsoft Office Memory Corruption Vulnerability, CVE-2017-11882 <https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2017-11882>	CCCS Alert Microsoft Office Security Update Microsoft Security Update Microsoft Security Update <https://www.cyber.gc.ca/en/alerts/microsoft-office-security-update>

Give Feedback

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2017-0199 < https://nvd.nist.gov/vuln/detail/cve-2017-0199 >	Microsoft	Multiple products; see Microsoft Security Update Guide: Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows, CVE-2017-0199 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2017-0199 >	Microsoft Security Update Guide: Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows, CVE-2017-0199 < https://msrc.microsoft.com/update-guide/en-us/vulnerability/cve-2017-0199 >	CCCS Microsoft Security Updates < https://www.cyber.gc.ca/en/alemts/microsoft-security-updates >

Give Feedback

Contact Information

U.S. organizations: Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to contact@mail.cisa.dhs.gov or by calling 1-844-Say-CISA (1-844-729-2472) and/or to the FBI via your local FBI field office <<https://www.fbi.gov/contact-us/field-offices>> 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

<<https://www.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: [<https://www.ncsc.gov.uk/section/about-this-website/contact-us>](http://ncsc.gov.uk/report-an-incident) (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Revisions

April 27, 2022: Initial Version

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

Give Feedback



Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

[Return to top](#)

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



CISA Central

1-844-Say-CISA

contact@cisa.dhs.gov



CISA.gov

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

[About CISA](#) </about>

[Budget and Performance](#)

[DHS.gov](https://www.dhs.gov) <https://www.dhs.gov>

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

[FOIA Requests](#)

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

[No FEAR Act](#) </no-fear-act>

[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>

Give Feedback