JOINT
CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-117A

April 27, 2022

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
Australian Cyber Security Centre
GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI
National Cyber Security Centre
a part of GCHQ

2021 Top Routinely Exploited Vulnerabilities

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), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), and United Kingdom's National Cyber Security Centre (NCSC-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.

***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.*

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 or earlier. The exploitation of older 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.
- **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: 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	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
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: CVE-2019-19781, CVE-2019-18935, and CVE-2017-11882.

Table 2: Additional Routinely Exploited Vulnerabilities in 2021

CVE	Vendor and Product	Type
CVE-2021-42237	Sitecore XP	RCE
CVE-2021-35464	ForgeRock OpenAM server	RCE
CVE-2021-27104	Accellion FTA	OS command execution
CVE-2021-27103	Accellion FTA	Server-side request forgery
CVE-2021-27102	Accellion FTA	OS command execution
CVE-2021-27101	Accellion FTA	SQL injection
CVE-2021-21985	VMware vCenter Server	RCE
CVE-2021-20038	SonicWall Secure Mobile Access (SMA)	RCE

CVE	Vendor and Product	Type
CVE-2021-40444	Microsoft MSHTML	RCE
CVE-2021-34527	Microsoft Windows Print Spooler	RCE
CVE-2021-3156	Sudo	Privilege escalation
CVE-2021-27852	Checkbox Survey	Remote arbitrary code execution
CVE-2021-22893	Pulse Secure Pulse Connect Secure	Remote arbitrary code execution
CVE-2021-20016	SonicWall SSLVPN SMA100	Improper SQL command neutralization, allowing for credential access
CVE-2021-1675	Windows Print Spooler	RCE
CVE-2020-2509	QNAP QTS and QuTS hero	Remote arbitrary code execution
CVE-2019-19781	Citrix Application Delivery Controller (ADC) and Gateway	Arbitrary code execution
CVE-2019-18935	Progress Telerik UI for ASP.NET AJAX	Code execution
CVE-2018-0171	Cisco IOS Software and IOS XE Software	Remote arbitrary code execution
CVE-2017-11882	Microsoft Office	RCE
CVE-2017-0199	Microsoft Office	RCE

MITIGATIONS

Vulnerability and Configuration Management

- Update software, operating systems, applications, and firmware on IT network assets in a timely manner. Prioritize patching known exploited vulnerabilities, 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.

- 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
    - 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

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).

Note: see CISA Capacity Enhancement Guide – Implementing Strong Authentication 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
- For the top exploited vulnerabilities 2016 through 2019, see joint CSA Top 10 Routinely Exploited Vulnerabilities.
- 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

APPENDIX: PATCH INFORMATION AND ADDITIONAL RESOURCES FOR TOP EXPLOITED VULNERABILITIES

CVE	Vendor	Affected Products	Patch Information	Resources
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 Exploitation of vulnerable Sitecore Experience Platform Content Management Systems
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	ACSC Advisory Active exploitation of ForgeRock Access Manager / OpenAM servers CCCS ForgeRock Security Advisory
CVE-2021-27104	Accellion	FTA 9_12_370 and earlier	Accellion Press Release: Update to Recent FTA Security Incident	Joint CSA Exploitation of Accellion File Transfer Appliance ACSC Alert Potential Accellion File Transfer Appliance compromise
CVE-2021-27103		FTA 9_12_411 and earlier		
CVE-2021-27102		FTA versions 9_12_411 and earlier		

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-27101		FTA 9_12_370 and earlier		
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	CCCS VMware Security Advisory
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	ACSC Alert VMware vCenter Server plugin remote code execution vulnerability CCCS VMware Security Advisory CCCS Alert APT Actors Target U.S. and Allied Networks - Update 1
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	ACSC Alert Remote code execution vulnerability present in SonicWall SMA 100 series appliances

CVE	Vendor	Affected Products	Patch Information	Resources
				CCCS 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.	Log4j: Apache Log4j Security Vulnerabilities For additional information, see joint CSA: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities	CISA webpage Apache Log4j Vulnerability Guidance CCCS Active exploitation of Apache Log4j vulnerability - Update 7
CVE-2021-40539	Zoho ManageEngine	ADSelfService Plus version 6113 and prior	Zoho ManageEngine: ADSelfService Plus 6114 Security Fix Release	Joint CSA APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus CCCS Zoho Security Advisory
CVE-2021-40444	Microsoft	Multiple Windows products; see Microsoft Security Update Guide: MSHTML Remote Code	Microsoft Security Update Guide: MSHTML Remote Code	

CVE	Vendor	Affected Products	Patch Information	Resources
		Execution Vulnerability, CVE-2021-40444	Execution Vulnerability, CVE-2021-40444	
CVE-2021-34527	Microsoft	Multiple Windows products; see Microsoft Security Update Guide: Windows Print Spooler Remote Code Execution Vulnerability, CVE-2021-34527	Microsoft Security Update Guide: Windows Print Spooler Remote Code Execution Vulnerability, CVE-2021-34527	Joint CSA Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability CCCS Alert Windows Print Spooler Vulnerability Remains Unpatched – Update 3
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	Joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2021-34473	Microsoft	Multiple Exchange Server versions; see: Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-34473	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-34473	ACSC Alert Microsoft Exchange ProxyShell Targeting in Australia
CVE-2021-31207	Microsoft	Multiple Exchange Server versions; see Microsoft Update Guide: Microsoft Exchange Server Security Feature Bypass Vulnerability, CVE-2021-31207	Microsoft Update Guide: Microsoft Exchange Server Security Feature Bypass Vulnerability, CVE-2021-31207	
CVE-2021-3156	Sudo	Sudo before 1.9.5p2	Sudo Stable Release 1.9.5p2	
CVE-2021-27852	Checkbox Survey	Checkbox Survey versions prior to 7		
CVE-2021-27065	Microsoft Exchange Server	Multiple versions; see: Microsoft Security Update Guide: Microsoft Exchange Server Remote Code	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code	CISA Alert: Mitigate Microsoft Exchange Server Vulnerabilities

CVE	Vendor	Affected Products	Patch Information	Resources
		Execution Vulnerability, CVE-2021-27065	Execution Vulnerability, CVE-2021-27065	ACSC Advisory Active exploitation of Vulnerable Microsoft Exchange servers CCCS Alert Active Exploitation of Microsoft Exchange Vulnerabilities - Update 4
CVE-2021-26858	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26858	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26858	
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	
CVE-2021-26855	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide: Microsoft Exchange Server Remote Code	Microsoft Security Update Guide: Microsoft Exchange Server Remote Code Execution Vulnerability, CVE-2021-26855	

CVE	Vendor	Affected Products	Patch Information	Resources
		Execution Vulnerability, CVE-2021-26855		
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	ACSC Alert Remote code execution vulnerability present in certain versions of Atlassian Confluence CCCS Atlassian Security Advisory
CVE-2021-22893	Pulse Secure	PCS 9.0R3/9.1R1 and Higher	Pulse Secure SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4	CCCS Alert Active Exploitation of Pulse Connect Secure Vulnerabilities - Update 1
CVE-2021-20016	SonicWall	SMA 100 devices (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v)	SonicWall Security Advisory SNWLID-2021-0001	
CVE-2021-1675	Microsoft	Multiple Windows products; see Microsoft Security Update Guide Windows Print Spooler	Microsoft Security Update Guide: Windows Print Spooler Remote Code Execution	CCCS Alert Windows Print Spooler Vulnerability Remains Unpatched – Update 3

CVE	Vendor	Affected Products	Patch Information	Resources
		Remote Code Execution Vulnerability, CVE-2021-1675	Vulnerability, CVE-2021-1675	
CVE-2020-2509	QNAP	QTS, multiple versions; see QNAP: Command Injection Vulnerability in QTS and QuTS hero QuTS hero h4.5.1.1491 build 20201119 and later	QNAP: Command Injection Vulnerability in QTS and QuTS hero	
CVE-2020-1472	Microsoft	Windows Server, multiple versions; see Microsoft Security Update Guide: Netlogon Elevation of Privilege Vulnerability, CVE-2020-1472	Microsoft Security Update Guide: Netlogon Elevation of Privilege Vulnerability, CVE-2020-1472	ACSC Alert Netlogon elevation of privilege vulnerability (CVE-2020-1472) Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations CCCS Alert Microsoft Netlogon Elevation of Privilege Vulnerability - CVE-2020-1472 - Update 1

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2020-0688	Microsoft	Exchange Server, multiple versions; see Microsoft Security Update Guide: Microsoft Exchange Validation Key Remote Code Execution Vulnerability, CVE-2020-0688	Microsoft Security Update Guide: Microsoft Exchange Validation Key Remote Code Execution Vulnerability, CVE-2020-0688	CISA Alert Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity Joint CSA Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology CCCS Alert Microsoft Exchange Validation Key Remote Code Execution Vulnerability
CVE-2019-19781	Citrix	ADC and Gateway version 13.0 all supported builds before 13.0.47.24 NetScaler ADC and NetScaler Gateway, version 12.1 all supported builds before	Citrix Security Bulletin CTX267027	Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations CISA Alert Chinese Ministry of State

CVE	Vendor	Affected Products	Patch Information	Resources
		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 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		Security-Affiliated Cyber Threat Actor Activity CCCS Alert Detecting Compromises relating to Citrix CVE-2019-19781
CVE-2019-18935	Progress Telerik	UI for ASP.NET AJAX through 2019.3.1023	Telerik UI for ASP.NET AJAX Allows JavaScriptSerializer Deserialization	ACSC Alert Active exploitation of vulnerability in Microsoft Internet Information Services
CVE-2019-11510	Pulse Secure	Pulse Connect Secure 8.2 before 8.2R12.1, 8.3	Pulse Secure: SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple	CISA Alert Continued Exploitation of Pulse

CVE	Vendor	Affected Products	Patch Information	Resources
		before 8.3R7.1, and 9.0 before 9.0R3.4	vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX	Secure VPN Vulnerability CISA Alert Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity ACSC Advisory Recommendations to mitigate vulnerability in Pulse Connect Secure VPN Software Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations CCCS Alert APT Actors Target U.S. and Allied Networks - Update 1
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	Joint CSA Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain

CVE	Vendor	Affected Products	Patch Information	Resources
				Sensitive U.S. Defense Information and Technology Joint CSA Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities Joint CSA APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations ACSC Alert APT exploitation of Fortinet Vulnerabilities CCCS Alert Exploitation of Fortinet FortiOS vulnerabilities (CISA, FBI) - Update 1

CVE	Vendor	Affected Products	Patch Information	Resources
CVE-2018-0171	Cisco	See Cisco Security Advisory: cisco-sa-20180328-smi2	Cisco Security Advisory: cisco-sa-20180328-smi2	CCCS Action Required to Secure the Cisco IOS and IOS XE Smart Install Feature
CVE-2017-11882	Microsoft	Office, multiple versions; see Microsoft Security Update Guide: Microsoft Office Memory Corruption Vulnerability, CVE-2017-11882	Microsoft Security Update Guide: Microsoft Office Memory Corruption Vulnerability, CVE-2017-11882	CCCS Alert Microsoft Office Security Update
CVE-2017-0199	Microsoft	Multiple products; see Microsoft Security Update Guide: Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows, CVE-2017-0199	Microsoft Security Update Guide: Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows, CVE-2017-0199	CCCS Microsoft Security Updates