National Security Agency | Cybersecurity Advisory

Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities

One of the greatest threats to U.S. National Security Systems (NSS), the U.S. Defense Industrial Base (DIB), and Department of Defense (DoD) information networks is Chinese state-sponsored malicious cyber activity. These networks often undergo a full array of tactics and techniques used by Chinese state-sponsored cyber actors to exploit computer networks of interest that hold sensitive intellectual property, economic, political, and military information. Since these techniques include exploitation of publicly known vulnerabilities, it is critical that network defenders prioritize patching and mitigation efforts.

The same process for planning the exploitation of a computer network by any sophisticated cyber actor is used by Chinese state-sponsored hackers. They often first identify a target, gather technical information on the target, identify any vulnerabilities associated with the target, develop or re-use an exploit for those vulnerabilities, and then launch their exploitation operation.

This advisory provides Common Vulnerabilities and Exposures (CVEs) known to be recently leveraged, or scanned-for, by Chinese state-sponsored cyber actors to enable successful hacking operations against a multitude of victim networks. Most of the vulnerabilities listed below can be exploited to gain initial access to victim networks using products that are directly accessible from the Internet and act as gateways to internal networks. The majority of the products are either for remote access (T1133)[1] or for external web services (T1190), and should be prioritized for immediate patching. While some vulnerabilities have specific additional mitigations below, the following mitigations generally apply:

- Keep systems and products updated and patched as soon as possible after patches are released.[2]
- Expect that data stolen or modified (including credentials, accounts, and software) before the device was patched will not be alleviated by patching, making password changes and reviews of accounts a good practice.
- Disable external management capabilities and set up an out-of-band management network.[3]
- Block obsolete or unused protocols at the network edge and disable them in device configurations.[4]
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce the exposure of the internal network.[5]
- Enable robust logging of Internet-facing services and monitor the logs for signs of compromise.[6]

Detailed Vulnerabilities and Mitigations

The following is a list of CVEs being actively used by Chinese state-sponsored cyber actors, a description of the vulnerability, and the recommended mitigations. (NOTE: The following list of CVEs is non-exhaustive of what is available or perhaps used by Chinese state-sponsored cyber actors, but is a list of those being operationalized by China.)

CVE Number	Vulnerability Description	Prior NSA Cybersecurity Guidance (Some focused on other actors)
CVE-2019-11510	***In Pulse Secure VPNs,® [7] an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability. This may lead to exposure of keys or passwords.***	CSA **–** Mitigating Recent VPN Vulnerabilities U/OO/196888-19 CSA **–** Advisory - APT29 target COVID-19 research organizations U/OO/152680-20
Affects: Pulse Connect Secure® (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4. [1]		

[1] T1190 and T1133 are MITRE® ATT&CK® techniques. MITRE and ATT&CK are registered trademarks of The MITRE Corporation.
[2] Refer to CSI – Update and Upgrade Software Immediately U/OO/181147-19
[3] Refer to CSI – Perform Out-of-Band Network Management U/OO/169570-20
[4] Refer to ORN – Outdated Software and Protocols Continue to Result in Endpoint and Network Compromise U/OO/802041-16
[5] Refer to CSI – Segment Networks and Deploy Application-Aware Defenses U/OO/184967-19
[6] Refer to CSI – Continuously Hunt for Network Intrusions U/OO/181860-19
[7] Pulse Secure VPN® is a registered trademark of Pulse Secure, LLC.

CVE Number	Vulnerability Description	Prior NSA Cybersecurity Guidance (Some focused on other actors)
Additional Mitigations: Note that patching does not address credentials which may have been lost prior to patches being applied. NSA discourages the use of proprietary SSLVPN/TLSVPN protocols, which are not compliant with CNSS policy. Transition SSLVPN/TLSVPN deployments to either IETF standard-conformant TLS for single application use cases, or to IKE/IPsec VPNs, preferably using one of the evaluated TLS software applications or IPSec VPN gateways/clients listed on the National Information Assurance Partnership (NIAP) Product Compliant List (PCL).		
CVE-2020-5902	***In F5 BIG-IP®[8] proxy / load balancer devices, the Traffic Management User Interface (TMUI) - also referred to as the Configuration utility - has a Remote Code Execution (RCE) vulnerability in undisclosed pages.***	CSI – Harden Network Devices U/OO/171339-16 CSI – Perform Out-of-Band Network Management U/OO/169570-20
Affects: F5 BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1. [2] **Additional Mitigations:** By default, the TMUI is accessible via the management interface on both the external and internal interface. Best practice is to disable the external interface and configure an out-of-band management network. NSA released guidance for this in the Harden Network Devices CSI (U/OO/171339-16) and the Perform Out-of-Band Network Management CSI (U/OO/169570-20).		
CVE-2019-19781	***An issue was discovered in Citrix®[9] Application Delivery Controller (ADC) and Gateway. They allow directory traversal, which can lead to remote code execution without credentials.***	CSI – Detect and Prevent Web Shell Malware U/OO/134094-20 CSA – Advisory - APT29 target COVID-19 research organizations U/OO/152680-20 CSA – Mitigate CVE-2019-19781 U/OO/103100-20
Affects: Citrix ADC and Gateway versions before 13.0.47.24, 12.1.55.18, 12.0.63.13, 11.1.63.15 and 10.5.70.12 and SD-WAN WANOP 4000-WO, 4100-WO, 5000-WO, and 5100-WO versions before 10.2.6b and 11.0.3b. [3]		
CVE-2020-8193 CVE-2020-8195 CVE-2020-8196	***Improper access control and input validation, in Citrix® ADC and Citrix® Gateway and Citrix® SDWAN WAN-OP, allows unauthenticated access to certain URL endpoints and information disclosure to low-privileged users.***	CSI – Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Citrix ADC and Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18, ADC FIPS versions before 12.1-55.179 and SD-WAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7. [4]		
CVE-2019-0708	***A remote code execution vulnerability exists within Remote Desktop Services®[10] when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests.***	CSA – Patch Remote Desktop Services on Legacy Versions of Windows U/OO/152674-19 ORN – Outdated Software and Protocols Continue to Result in Endpoint and Network Compromise U/OO/802041-16
Affects: Microsoft Windows®[11] XP - 7, Microsoft Windows Server®[12] 2003 - 2008. **Additional Mitigations:** Block TCP Port 3389 at your firewalls, especially any perimeter firewalls exposed to the internet. This port is used by the Remote Desktop Protocol (RDP) and will block attempts to establish a connection. Disable Remote Desktop Services if they are not required. Disabling unused and unneeded services helps reduce exposure to security vulnerabilities overall and is a best practice even without the BlueKeep threat. Enable Network Level Authentication. With NLA enabled, attackers would first have to authenticate to RDS in order to successfully exploit the vulnerability. NLA is available on the Windows® 7, Windows Server® 2008 and Windows Server® 2008 R2 operating systems.		
CVE-2020-15505	***A remote code execution vulnerability in the MobileIron®[13] mobile device management (MDM)***	CSI – Update and Upgrade Software Immediately U/OO/181147-19

[8] F5 BIG-IP® is a registered trademark of F5 Networks, Inc.

[9] Citrix® is a registered trademark of Citrix Systems, Inc.

[10] Remote Desktop Services® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

[11] Windows OS® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

[12] Windows Server® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

[13] MobileIron® is a registered trademark of MobileIron, Inc.

CVE Number	Vulnerability Description	Prior NSA Cybersecurity Guidance (Some focused on other actors)
	software that allows remote attackers to execute arbitrary code via unspecified vectors.	
Affects: MobileIron® Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier. [5]		
CVE-2020-1350	***A remote code execution vulnerability exists in Windows® Domain Name System servers when they fail to properly handle requests.***	CSA **–** Patch Critical Vulnerability in Windows Servers® using DNS Server Role U/OO/152726-20
Affects: Microsoft Windows Server® 2008 - 2019 **Additional Mitigations:** Keep system and product updated and patched. In the event that an update cannot be applied immediately, the following workaround will prevent the vulnerability from being exploited, per Microsoft's® recommendation. The workaround configures Windows® DNS servers to restrict the size of acceptable DNS message packets over TCP to 65,280 bytes (0xFF00). Applying the workaround requires a restart of the DNS service. Apply the patch as soon as possible and remove the workaround once the patch is applied. Launch an elevated PowerShell prompt: ***Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters -Name TcpReceivePacketSize -Type DWord -Value 0xFF00***		
CVE-2020-1472	***An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19
Affects: Microsoft Windows Server® 2008 - 2019 **Additional Mitigations:** Install the patch and implement the additional instructions found in Microsoft article KB4557222.		
CVE-2019-1040	***A tampering vulnerability exists in Microsoft Windows® when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19 ORN – Outdated Software and Protocols Continue to Result in Endpoint and Network Compromise U/OO/802041-16
Affects: Microsoft Windows® 7 - 10, Microsoft Windows Server® 2008 - 2019. **Additional Mitigations:** Limit the use of NTLM as much as possible and stop the use of NTLMv1. [6] [7]		
CVE-2018-6789	***Sending a handcrafted message to Exim mail transfer agent may cause a buffer overflow. This can be used to execute code remotely.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19
Affects: Exim before 4.90.1. [8]		
CVE-2020-0688	***A Microsoft Exchange® validation key remote code execution vulnerability exists when the software fails to properly handle objects in memory.***	CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Microsoft Exchange Server® 2010 Service Pack 3 Update Rollup 29 and earlier, 2013 Cumulative Update 22 and earlier, 2016 Cumulative Update 13 and earlier and 2019 Cumulative Update 2 and earlier. [9]		
CVE-2018-4939	***Certain Adobe ColdFusion®[14] versions have an exploitable Deserialization of Untrusted Data vulnerability. Successful exploitation could lead to arbitrary code execution.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19
Affects: Adobe ColdFusion (2016 release) Update 5 and earlier versions, ColdFusion 11 Update 13 and earlier versions. [10]		
CVE-2015-4852	***The WLS Security component in Oracle WebLogic®[15] Server allows remote attackers to execute arbitrary commands via a crafted serialized Java®[16] object.***	CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0. [11]		
CVE-2020-2555	***A vulnerability exists in the Oracle® Coherence product of Oracle Fusion® Middleware. This easily exploitable***	CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20

[14] Adobe ColdFusion® is a registered trademark of Adobe Systems, Inc.

[15] Oracle WebLogic® is a registered trademark of Oracle Corporation.

[16] Java® is a registered trademark of Oracle Corporation.

CVE Number	Vulnerability Description	Prior NSA Cybersecurity Guidance (Some focused on other actors)
	vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle® Coherence.	
Affects: Oracle Coherence 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. [12]		
[CVE-2019-3396](#)	***The Widget Connector macro in Atlassian Confluence®[17] Server allows remote attackers to achieve path traversal and remote code execution on a Confluence® Server or Data Center instance via server-side template injection.***	CSA **–** Patch Critical Vulnerability In Atlassian Confluence CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Atlassian Confluence before 6.6.12, 6.7.0 to before 6.12.3, 6.13.0 to before 6.13.3, and 6.14.0 to before 6.14.2. [13]		
[CVE-2019-11580](#)	***Attackers who can send requests to an Atlassian® Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits remote code execution.***	CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Atlassian Crowd from 2.1.0 to before 3.0.5, 3.1.0 to before 3.1.6, 3.2.0 to before 3.2.8, 3.3.0 to before 3.3.5, and 3.4.0 to before 3.4.4. [14]		
[CVE-2020-10189](#)	***Zoho ManageEngine®[18] Desktop Central allows remote code execution because of deserialization of untrusted data.***	CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Zoho ManageEngine Desktop Central before 10.0.479. [15]		
[CVE-2019-18935](#)	***Progress Telerik®[19] UI for ASP.NET AJAX contains a .NET deserialization vulnerability. Exploitation can result in remote code execution.***	CSI **–** Detect and Prevent Web Shell Malware U/OO/134094-20
Affects: Progress Telerik UI for ASP.NET AJAX through 2019.3.1023. [16] **Additional Mitigations:** NSA concurs with Tenable's®[20] recommendations: "This is exploitable when the encryption keys are known due to the presence of CVE-2017-11317 or CVE-2017-11357, or other means. Exploitation can result in remote code execution. (As of 2020.1.114, a default setting prevents the exploit. In 2019.3.1023, but not earlier versions, a non-default setting can prevent exploitation.)" [16]		
[CVE-2020-0601](#)	***A spoofing vulnerability exists in the way Windows® CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear that the file was from a trusted, legitimate source.***	CSA **–** Patch Critical Cryptographic Vulnerability in Microsoft Windows® Clients and Servers U/OO/104201-20
Affects: Microsoft Windows® 10, Server® 2016 - 2019. **Additional Mitigations:** In addition, the Windows® certificate utility (certutil) and the OpenSSL®[21] utility can be used to inspect a certificate for explicitly defined or non-standard elliptic curve parameters if a suspect certificate is encountered.		
[CVE-2019-0803](#)	***An elevation of privilege vulnerability exists in Windows® when the Win32k component fails to properly handle objects in memory.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19
Affects: Microsoft Windows® 7 - 10, Microsoft Windows Server® 2008 - 2019.		
[CVE-2017-6327](#)	***The Symantec®[22] Messaging Gateway can encounter a remote code execution issue.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19
Affects: Symantec Messaging Gateway before 10.6.3-267. [17] **Additional Mitigations:** Run under the principle of least privilege, where possible, to limit the impact of potential exploit.		
[CVE-2020-3118](#)	***A vulnerability in the Cisco® Discovery Protocol implementation for Cisco IOS®[23] XR Software could allow***	CSI **–** Harden Network Devices U/OO/171339-16

[17] Atlassian Confluence® is a registered trademark of Atlassian, Inc.
[18] ManageEngine® is a registered trademark of Zoho Corporation.
[19] Telerik UI® is a registered trademark of Telerik AD.
[20] Tenable® is a registered trademark of Tenable, Inc.
[21] OpenSSL® is a registered trademark of OpenSSL Software Foundation.
[22] Symantec® is a registered trademark of Broadcom Corporation.
[23] Cisco IOS® is a registered trademark of Cisco Systems, Inc. in the United States and other countries.

CVE Number	Vulnerability Description	Prior NSA Cybersecurity Guidance (Some focused on other actors)
	an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device.	
Affects: Cisco IOS XR 5.2.5, 6.5.2, 6.5.3, 6.6.25, 7.0.1. [18] **Additional Mitigations:** On many devices, Cisco® Discovery Protocol is enabled by default. NSA recommends disabling discovery protocols, per our Harden Network Devices CSI. To determine if CDP is enabled, use the “show running-config | include cdp” command.		
CVE-2020-8515	***DrayTek Vigor®[24] devices allow remote code execution as root (without authentication) via shell metacharacters.***	CSI – Update and Upgrade Software Immediately U/OO/181147-19
Affects: Vigor2960® 1.3.1_Beta, Vigor3900® 1.4.4_Beta, and Vigor300B® 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices. [19] **Additional Mitigations:** After patching the system, check to make sure that no additional admin users or remote access profiles have been added. Verify that no changes have been made to Access Control Lists.		

NSA is aware that National Security Systems, Defense Industrial Base, and Department of Defense networks are consistently scanned, targeted, and exploited by Chinese state-sponsored cyber actors. NSA recommends that critical system owners consider these actions a priority, in order to mitigate the loss of sensitive information that could impact U.S. policies, strategies, plans, and competitive advantage. Additionally, due to the various systems and networks that could be impacted by the information in this product outside of these sectors, NSA recommends that the CVEs above be prioritized for action by all network defenders.

Works Cited

[1] “SA44101 – 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure® / Pulse Policy Secure 9.0RX.” PulseSecure®, 07 August 2020. [Online] Available: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101 [Accessed 22 September 2020]

[2] “K52145254: TMUI RCE vulnerability CVE-2020-5902.”F5, 22 July 2020. [Online] Available at: https://support.f5.com/csp/article/K52145254 [Accessed 22 September 2020]

[3] “Citrix® | Support Knowledge Center: CTX267027 CVE-2019-19781 - Vulnerability in Citrix® Application Delivery Controller, Citrix® Gateway, and Citrix SD-WAN WANOP appliance.” Citrix®, 24 Jan 2020. [Online] Available at: https://support.citrix.com/article/CTX267027 [Accessed 21 September 2020]

[4] “Citrix® | Support Knowledge Center: CTX276688 Citrix® Application Delivery Controller, Citrix® Gateway, and Citrix® SDWAN WANOP appliance Security Update.” Citrix, 17 Aug 2020. [Online] Available at: https://support.citrix.com/article/CTX276688 [Accessed 21 September 2020]

[5] “MobileIron® Security Updates Available.” MobileIron®, 01 July 2020. [Online] Available: https://www.mobileiron.com/en/blog/mobileiron-security-updates-available [Accessed 22 September 2020]

[6] “Stop using LAN Manager and NTLMv1.” Microsoft®, 7 Nov 2017. [Online] Available at: https://blogs.technet.microsoft.com/miriamxyra/2017/11/07/stop-using-lan-manager-and-ntlmv1 [Accessed 22 September 2020]

[7] “Network security: Restrict NTLM: Audit NTLM authentication in this domain.” Microsoft®, 19 Apr 2017. [Online] Available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-audit-ntlm-authentication-in-this-domain [Accessed 22 September 2020]

[8] “CVE Details: Vulnerability Details: CVE-2018-6789.” CVE Details, 26 Oct 2018. [Online] Available at: https://www.cvedetails.com/cve/CVE-2018-6789/ [Accessed 18 September 2020]

[9] “CVE-2020-0688 | Microsoft Exchange® Validation Key Remote Code Execution Vulnerability.” Microsoft®, 11 Feb. 2020. [Online] Available at: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688 [Accessed 18 September 2020]

[10] “Adobe® Security Bulletin: Security updates available for Cold Fusion® | APSB18-14.” Adobe, 10 Apr 2018. [Online] Available at: https://helpx.adobe.com/security/products/coldfusion/apsb18-14.html [Accessed 18 September 2020]

[11] “Oracle®[25] Security Alert for CVE-2015-4852.” Oracle®, 12 Nov 2015. [Online] Available at: https://www.oracle.com/security-alerts/alert-cve-2015-4852.html [Accessed 23 September 2020]

[12] “Confluence® Security Advisory - 201903-20: March 2019 Confluence® Server Advisory - WebDAV and Widget Connector vulnerabilities.” Atlassian®, 20 Mar 2019. [Online] Available at: https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html [Accessed 18 September 2020]

[24] DrayTek Vigor® is a registered trademark of Draytek Corp.

[25] Oracle® is a registered trademark of Oracle Corporation.

[13] "Crowd Security Advisory 2019-05-22: Crowd: pdkinstall development plugin incorrectly enabled (CVE-2019-11580)." Atlassian® 23 May 2019. [Online] Available at: https://confluence.atlassian.com/crowd/crowd-security-advisory-2019-05-22-970260700.html [Accessed 21 September 2020]

[14] "ManageEngine® Desktop Central remote code execution vulnerability (CVE-2020-10189)." ManageEngine®. [Online] Available at: https://www.manageengine.com/products/desktop-central/remote-code-execution-vulnerability.html [Accessed 21 September 2020]

[15] "Tenable®: https://www.tenable.com/cve/CVE-2019-18935." Tenable®, 16 Jan 2020. [Online] Available at: https://www.tenable.com/cve/CVE-2019-18935 [Accessed 23 September 2020]

[16] "Symantec® Messaging Gateway RCE and CSRF." Broadcom®, 05 March 2020. [Online database entry] Available at: https://support.broadcom.com/security-advisory/content/0/0/SYMSA1411 [Accessed 22 September 2020]

[17] "Cisco IOS® XR Software Discovery Protocol Format String Vulnerability." Cisco®, 05 February, 2020. [Online] Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa20200205-iosxr-cdp-rce [Accessed 22 September 2020

[18] "Vigor3900® / Vigor2960® / Vigor300B® Router Web Management Page Vulnerability (CVE-2020-8515)." DrayTek®, 10 February 2020. [Online] Available: https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov