Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors

cisa.gov/uscert/ncas/alerts/aa22-279a

Summary

This joint Cybersecurity Advisory (CSA) provides the top Common Vulnerabilities and Exposures (CVEs) used since 2020 by People's Republic of China (PRC) state-sponsored cyber actors as assessed by the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI). PRC state-sponsored cyber actors continue to exploit known vulnerabilities to actively target U.S. and allied networks as well as software and hardware companies to steal intellectual property and develop access into sensitive networks.

This joint CSA builds on previous NSA, CISA, and FBI reporting to inform federal and state, local, tribal and territorial (SLTT) government; critical infrastructure, including the Defense Industrial Base Sector; and private sector organizations about notable trends and persistent tactics, techniques, and procedures (TTPs).

NSA, CISA, and FBI urge U.S. and allied governments, critical infrastructure, and private sector organizations to apply the recommendations listed in the Mitigations section and Appendix A to increase their defensive posture and reduce the threat of compromise from PRC state-sponsored malicious cyber actors.

For more information on PRC state-sponsored malicious cyber activity, see CISA's China Cyber Threat Overview and Advisories webpage, FBI's Industry Alerts, and NSA's Cybersecurity Advisories & Guidance.

Download the PDF version of this report: pdf, 409 KB

Technical Details

NSA, CISA, and FBI continue to assess PRC state-sponsored cyber activities as being one of the largest and most dynamic threats to U.S. government and civilian networks. PRC state-sponsored cyber actors continue to target government and critical infrastructure networks with an increasing array of new and adaptive techniques—some of which pose a significant risk to Information Technology Sector organizations (including telecommunications providers), Defense Industrial Base (DIB) Sector organizations, and other critical infrastructure organizations.

PRC state-sponsored cyber actors continue to exploit known vulnerabilities and use publicly available tools to target networks of interest. NSA, CISA, and FBI assess PRC state-sponsored cyber actors have actively targeted U.S. and allied networks as well as software and hardware companies to steal intellectual property and develop access into sensitive networks. See Table 1 for the top used CVEs.

Table I: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitrary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Execution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitrary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal

Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution
Apache HTTP Server	CVE-2021-41773	Path Traversal

These state-sponsored actors continue to use virtual private networks (VPNs) to obfuscate their activities and target web-facing applications to establish initial access. Many of the CVEs indicated in Table 1 allow the actors to surreptitiously gain unauthorized access into sensitive networks, after which they seek to establish persistence and move laterally to other internally connected networks. For additional information on PRC state-sponsored cyber actors targeting network devices, please see People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices.

Mitigations

NSA, CISA, and FBI urge organizations to apply the recommendations below and those listed in Appendix A.

- Update and patch systems as soon as possible. Prioritize patching vulnerabilities identified in this CSA and other known exploited vulnerabilities.
- Utilize phishing-resistant multi-factor authentication whenever possible. Require all accounts with password logins to have strong, unique passwords, and change passwords immediately if there are indications that a password may have been compromised.
- Block obsolete or unused protocols at the network edge.
- Upgrade or replace end-of-life devices.
- Move toward the Zero Trust security model.
- Enable robust logging of Internet-facing systems and monitor the logs for anomalous activity.

Appendix A

Table II: Apache CVE-2021-44228

Apache CVE-2021-44228 CVSS 3.0: 10 (Critical)

Vulnerability Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against malicious actor controlled LDAP and other JNDI related endpoints. A malicious actor who can control log messages or log message parameters could execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Recommended Mitigations

Apply patches provided by vendor and perform required system updates.

Detection Methods

See vendor's Guidance For Preventing, Detecting, and Hunting for Exploitation of the Log4j 2 Vulnerability.

Vulnerable Technologies and Versions

There are numerous vulnerable technologies and versions associated with CVE-2021-44228. For a full list, check https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

Table III: Pulse CVE-2019-11510

Pulse CVE-2019-11510 CVSS 3.0: 10 (Critical)

Vulnerability Description

This vulnerability has been modified since it was last analyzed by NVD. It is awaiting reanalysis, which may result in further changes to the information provided. InPulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote malicious actor could send a specially crafted URI to perform an arbitrary file reading vulnerability.

Recommended Mitigations

Apply patches provided by vendor and perform required system updates.

Detection Methods

Use CISA's "Check Your Pulse" Tool.

Vulnerable Technologies and Versions

Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4

Table IV: GitLab CVE-2021-22205

GitLab CVE-2021-22205 CVSS 3.0: 10 (Critical)

Vulnerability Description

An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files passed to a file parser, which resulted in a remote command execution.

Recommended Mitigations

- Update to 12.10.3, 13.9.6, and 13.8.8 for GitLab.
- Hotpatch is available via GitLab.

Detection Methods

- Investigate logfiles.
- Check GitLab Workhorse.

Vulnerable Technologies and Versions

Gitlab CE/EE.

Table V: Atlassian CVE-2022-26134

Atlassian CVE-2022-26134 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that could allow an unauthenticated malicious actor to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, 7.13.0 before 7.13.7, 7.14.0 before 7.14.3, 7.15.0 before 7.15.2, 7.16.0 before 7.16.4, 7.17.0 before 7.17.4, and 7.18.0 before 7.18.1.

Recommended Mitigations

> Immediately block all Internet traffic to and from affected products AND apply the update per vendor instructions.

- Ensure Internet-facing servers are up-to-date and have secure compliance practices.
- Short term workaround is provided here.

Detection Methods

N/A

Vulnerable Technologies and Versions

All supported versions of Confluence Server and Data Center

Confluence Server and Data Center versions after 1.3.0

Table VI: Microsoft CVE-2021-26855

Microsoft CVE-2021-26855	**CVSS 3.0: 9.8 (Critical)**

Vulnerability Description

Microsoft has released security updates for Windows Exchange Server. To exploit these vulnerabilities, an authenticated malicious actor could send malicious requests to an affected server. A malicious actor who successfully exploited these vulnerabilities would execute arbitrary code and compromise the affected systems. If successfully exploited, these vulnerabilities could allow an adversary to obtain access to sensitive information, bypass security restrictions, cause a denial of service conditions, and/or perform unauthorized actions on the affected Exchange server, which could aid in further malicious activity.

Recommended Mitigations

- Apply the appropriate Microsoft Security Update.
- Microsoft Exchange Server 2013 Cumulative Update 23 (KB5000871)
- Microsoft Exchange Server 2016 Cumulative Update 18 (KB5000871)
- Microsoft Exchange Server 2016 Cumulative Update 19 (KB5000871)
- Microsoft Exchange Server 2019 Cumulative Update 7 (KB5000871)
- Microsoft Exchange Server 2019 Cumulative Update 8 (KB5000871)
- Restrict untrusted connections.

Detection Methods

- Analyze Exchange product logs for evidence of exploitation.
- Scan for known webshells.

Vulnerable Technologies and Versions

Microsoft Exchange 2013, 2016, and 2019.

Table VII: F5 CVE-2020-5902

F5 CVE-2020-5902	**CVSS 3.0: 9.8 (Critical)**

Vulnerability Description

In 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, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

Recommended Mitigations

- Apply FY BIG-IP Update.
- Restrict access to the configuration utility.

Detection Methods

- Use F5's CVE-2020-5902 IoC Detection Tool.
- Additional detection methods can be found at https://support.f5.com/csp/article/K52145254.

Vulnerable Technologies and Versions

F5 Big-IP Access Policy Manager

F5 Big-IP Advanced Firewall Manager

F5 Big-IP Advanced Web Application Firewall

F5 Big-IP Analytics

F5 Big-IP Application Acceleration Manager

F5 Big-IP Application Security Manager

F5 Big-IP Ddos Hybrid Defender

F5 Big-IP Domain Name System (DNS)

F5 Big-IP Fraud Protection Service (FPS)

F5 Big-IP Global Traffic Manager (GTM)

F5 Big-IP Link Controller

F5 Networks Big-IP Local Traffic Manager (LTM)

F5 Big-IP Policy Enforcement Manager (PEM)

F5 SSL Orchestrator

References

https://support.f5.com/csp/article/K00091341

https://support.f5.com/csp/article/K07051153

https://support.f5.com/csp/article/K20346072

https://support.f5.com/csp/article/K31301245

https://support.f5.com/csp/article/K33023560

https://support.f5.com/csp/article/K43638305

https://support.f5.com/csp/article/K52145254

https://support.f5.com/csp/article/K82518062

Table VIII: VMware CVE-2021-22005

VMware CVE-2021-22005 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file.

Recommended Mitigations

Apply Vendor Updates.

Detection Methods

N/A

Vulnerable Technologies and Versions

VMware Cloud Foundation

VMware VCenter Server

Table IX: Citrix CVE-2019-19781

Citrix CVE-2019-19781 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

This vulnerability has been modified since it was last analyzed by NVD. It is awaiting reanalysis, which may result in further changes to the information provided. An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.

Recommended Mitigations

- Apply vendor mitigations.
- Use the CTX269180 - CVE-2019-19781 Verification Tool provided by Citrix.

Detection Methods

N/A

Vulnerable Technologies and Versions

Citrix ADC, Gateway, and SD-WAN WANOP

Table X: Cisco CVE-2021-1497

Cisco CVE-2021-1497 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote malicious actor to perform a command injection against an affected device. For more information about these vulnerabilities, see the Technical details section of this advisory.

Recommended Mitigations

Apply Cisco software updates.

Detection Methods

Look at the Snort Rules provided by Cisco.

Vulnerable Technologies and Versions

Cisco Hyperflex Hx Data Platform 4.0(2A)

Table XI: Buffalo CVE-2021-20090

Buffalo CVE-2021-20090 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

A path traversal vulnerability in the web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 could allow unauthenticated remote malicious actors to bypass authentication.

Recommended Mitigations

Update firmware to latest available version.

Detection Methods

N/A

Vulnerable Technologies and Versions

Buffalo Wsr-2533Dhpl2-Bk Firmware

Buffalo Wsr-2533Dhp3-Bk Firmware

Table XII: Atlassian CVE-2021-26084

Atlassian CVE-2021-26084 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated malicious actor to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are before version 6.13.23 and from version 6.14.0 before 7.4.11, version 7.5.0 before 7.11.6, and version 7.12.0 before 7.12.5.

Recommended Mitigations

- Update confluence version to 6.13.23, 7.4.11, 7.11.6, 7.12.5, and 7.13.0.
- Avoid using end-of-life devices.
- Use Intrusion Detection Systems (IDS).

Detection Methods

N/A

Vulnerable Technologies and Versions

Atlassian Confluence

Atlassian Confluence Server

Atlassian Data Center

Atlassian Jira Data Center

Table XIII: Hikvision CVE-2021-36260

Hikvision CVE-2021-36260 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

This vulnerability has been modified since it was last analyzed by NVD. It is awaiting reanalysis, which may result in further changes to the information provided. A command injection vulnerability exists in the web server of some Hikvision products. Due to the insufficient input validation, a malicious actor can exploit the vulnerability to launch a command injection by sending some messages with malicious commands.

Recommended Mitigations

Apply the latest firmware updates.

Detection Methods

N/A

Vulnerable Technologies and Versions

Various Hikvision Firmware to include Ds, Ids, and Ptz

References

https://www.cisa.gov/uscert/ncas/current-activity/2021/09/28/rce-vulnerability-hikvision-cameras-cve-2021-36260

Table XIV: Sitecore CVE-2021-42237

Sitecore CVE-2021-42237 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7 is vulnerable to an insecure deserialization attack where it is possible to achieve remote command execution on the machine. No authentication or special configuration is required to exploit this vulnerability.

Recommended Mitigations

- Update to latest version.
- Delete the Report.ashx file from /sitecore/shell/ClientBin/Reporting/Report.ashx.

Detection Methods

N/A

Vulnerable Technologies and Versions

Sitecore Experience Platform 7.5, 7.5 Update 1, and 7.5 Update 2

Sitecore Experience Platform 8.0, 8.0 Service Pack 1, and 8.0 Update 1-Update 7

Sitecore Experience Platform 8.0 Service Pack 1

Sitecore Experience Platform 8.1, and Update 1-Update 3

Sitecore Experience Platform 8.2, and Update 1-Update 7

Table XV: F5 CVE-2022-1388

F5 CVE-2022-1388 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

This vulnerability has been modified since it was last analyzed by NVD. It is awaiting reanalysis, which may result in further changes to the information provided. On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

Recommended Mitigations

- Block iControl REST access through the self IP address.
- Block iControl REST access through the management interface.
- Modify the BIG-IP httpd configuration.

Detection Methods

N/A

Vulnerable Technologies and Versions

Big IP versions:

16.1.0-16.1.2

15.1.0-15.1.5

14.1.0-14.1.4

13.1.0-13.1.4

12.1.0-12.1.6

11.6.1-11.6.5

Table XVI: Apache CVE-2022-24112

Apache CVE-2022-24112 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

A malicious actor can abuse the batch-requests plugin to send requests to bypass the IP restriction of Admin API. A default configuration of Apache APISIX (with default API key) is vulnerable to remote code execution. When the admin key was changed or the port of Admin API was changed to a port different from the data panel, the impact is lower. But there is still a risk to bypass the IP restriction of Apache APISIX's data panel. There is a check in the batch-requests plugin which overrides the client IP with its real remote IP. But due to a bug in the code, this check can be bypassed.

Recommended Mitigations

In affected versions of Apache APISIX, you can avoid this risk by explicitly commenting out batch-requests in the conf/config.yaml and conf/config-default.yaml files and restarting Apache APISIX.

Update to 2.10.4 or 2.12.1.

Detection Methods

N/A

Vulnerable Technologies and Versions

Apache APISIX between 1.3 and 2.12.1 (excluding 2.12.1)

LTS versions of Apache APISIX between 2.10.0 and 2.10.4

Table XVII: ZOHO CVE-2021-40539

ZOHO CVE-2021-40539 CVSS 3.0: 9.8 (Critical)

Vulnerability Description

Zoho ManageEngine ADSelfService Plus version 6113 and prior is vulnerable to REST API authentication bypass with resultant remote code execution.

Recommended Mitigations

Upgrade to latest version.

Detection Methods

- Run ManageEngine's detection tool.
- Check for specific files and logs.

Vulnerable Technologies and Versions

Zoho Corp ManageEngine ADSelfService Plus

Table XVIII: Microsoft CVE-2021-26857

Microsoft CVE-2021-26857 CVSS 3.0: 7.8 (High)

Vulnerability Description

Microsoft Exchange Server remote code execution vulnerability. This CVE ID differs from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, and CVE-2021-27078.

Recommended Mitigations

- Update to support latest version.
- Install Microsoft security patch.
- Use Microsoft Exchange On-Premises Mitigation Tool.

Detection Methods

- Run Exchange script: https://github.com/microsoft/CSS-Exchange/tree/main/Security.
- Hashes can be found here: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/#scan-log.

Vulnerable Technologies and Versions

Microsoft Exchange Servers

Table XIX: Microsoft CVE-2021-26858

Microsoft CVE-2021-26858 CVSS 3.0: 7.8 (High)

Vulnerability Description

Microsoft Exchange Server remote code execution vulnerability. This CVE ID differs from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, and CVE-2021-27078.

Recommended Mitigations

- Update to support latest version.
- Install Microsoft security patch.
- Use Microsoft Exchange On-Premises Mitigation Tool.

Detection Methods

- Run Exchange script: https://github.com/microsoft/CSS-Exchange/tree/main/Security.
- Hashes can be found here: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/#scan-log.

Vulnerable Technologies and Versions

Microsoft Exchange Servers

Table XX: Microsoft CVE-2021-27065

Microsoft CVE-2021-27065 CVSS 3.0: 7.8 (High)

Vulnerability Description

Microsoft Exchange Server remote code execution vulnerability. This CVE ID differs from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, and CVE-2021-27078.

Recommended Mitigations

- Update to support latest version.
- Install Microsoft security patch.
- Use Microsoft Exchange On-Premises Mitigation Tool.

Detection Methods

- Run Exchange script: https://github.com/microsoft/CSS-Exchange/tree/main/Security.
- Hashes can be found here: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/#scan-log.

Vulnerable Technologies and Versions

Microsoft Exchange Servers

References

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27065

Table XXI: Apache CVE-2021-41773

Apache CVE-2021-41773 CVSS 3.0: 7.5 (High)

Vulnerability Description

This vulnerability has been modified since it was last analyzed by NVD. It is awaiting reanalysis, which may result in further changes to the information provided. A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. A malicious actor could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied," these requests can succeed. Enabling CGI scripts for these aliased paths could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 is incomplete (see CVE-2021-42013).

Recommended Mitigations

Apply update or patch.

Detection Methods

Commercially available scanners can detect CVE.

Vulnerable Technologies and Versions

Apache HTTP Server 2.4.49 and 2.4.50

Fedoraproject Fedora 34 and 35

Oracle Instantis Enterprise Track 17.1-17.3

Netapp Cloud Backup

Revisions

Initial Publication: October 6, 2022

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.