



THREAT ADVISORY

**ATTACK
REPORT**

**Network Providers and Devices targeted by
Chinese state sponsored actors**

Date of Publication

8 June 2022

Admiralty code

A1

TA Number








TA2022114





Summary

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) has released a joint advisory to make organizations in telecommunications industry aware about the People's Republic of China (PRC) state-sponsored cyber actors that are continuing its behavior to exploit publicly known vulnerabilities in network devices.

CVEs

CVE	NAME	PATCH
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	
CVE-2019-15271	Cisco Small Business RV016, RV042, RV042G, and RV082 Routers Arbitrary Command Execution Vulnerability	
CVE-2019-1652	Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability	
CVE-2019-19781	Vulnerability in Citrix products leading to arbitrary code execution	

CVE	NAME	PATCH
CVE-2020-8515	Vigor Router Web Management Page Vulnerability	
CVE-2019-16920	D-Link DIR-866L Unauthenticated RCE Vulnerability	
CVE-2018-13382	Unauthenticated SSL VPN user's password modification Vulnerability	
CVE-2018-14847	MicroTik RouterOS Remote Rooting Vulnerability	
CVE-2017-6862	Unauthenticated Remote Code Execution vulnerability in NETGEAR Routers	
CVE-2021-22893	Use After Free vulnerability in Pulse Connect Secure	
CVE-2019-7193	An improper input validation vulnerability in QNAP NAS devices	

CVE	NAME	PATCH
CVE-2019-7192	An improper access control vulnerability in QNAP NAS devices	
CVE-2019-7194	An external control of file name or path vulnerability in QNAP NAS devices	
CVE-2019-7195	An external control of file name or path vulnerability in QNAP NAS devices	
CVE-2020-29583	A hardcoded credential vulnerability of firewalls and AP controllers	

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0043 Reconnaissance	TA0011 Command and Control	TA0007 Discovery
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0010 Exfiltration
TA0006 Credential Access	TA0009 Collection	T1078 Valid Accounts	T1119 Automated Collection
T1595 Active Scanning	T1595.002 Active Scanning: Vulnerability Scanning	T1133 External Remote Services	T1599 Network Boundary Bridging
T1190 Exploit Public-Facing Application	T1572 Protocol Tunneling	T1020 Automated Exfiltration	T1020.001 Automated Exfiltration: Traffic Duplication
T1555 Credentials from Password Stores	T1016 System Network Configuration Discovery	T1016.001 System Network Configuration Discovery: Internet Connection Discovery	

Technical Details

#1

Since 2020, People's Republic of China(PRC) state-sponsored attackers have started widespread campaigns to rapidly exploit publicly disclosed security flaws.

#2

They typically begin campaigns by scanning network devices for vulnerabilities using publicly available tools such as RouterSploit and RouterScan. Following that, they get access to these susceptible devices and locate a vital Remote Authentication Dial-In User Service (RADIUS) server. This allowed the threat actor to get access to the underlying Structured Query Language (SQL) database and dump the credentials, which included both cleartext and hashed passwords for user and administrative accounts. The credentials obtained are also used to authenticate routers and modify network traffic, allowing the threat actor to exfiltrate data from victims to their infrastructure.

#3

Some of the mitigation's organizations can apply:

- Keep systems and devices up to date and patched as soon as fixes are released.
- Remove or isolate suspected infected devices from the network immediately.
- Disable any network services, ports, protocols, or devices that are no longer in use.
- Implement multifactor authentication (MFA) requirement for all users.
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to limit internal network exposure.
- Limit or prevent lateral movement by segmenting networks.

🌀 Patch Links

<http://www.zyxel.com/support/CVE-2020-29583.shtml>

<http://www.qnap.com/zh-tw/security-advisory/nas-201911-25>

http://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/p?pubstatus=o

<https://kb.netgear.com/000038542/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-Some-Routers-PSV-2016-0261>

<https://forum.mikrotik.com/viewtopic.php?f=21&t=133533>

<https://www.fortiguard.com/psirt/FG-IR-18-389>

[http://www.draytek.com/about/security-advisory/vigor3900/-/vigor2960/-/vigor300b-router-web-management-page-vulnerability-\(cve-2020-8515\)/](http://www.draytek.com/about/security-advisory/vigor3900/-/vigor2960/-/vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/)

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-info>

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2>

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

🌀 References

<https://www.cisa.gov/uscert/ncas/alerts/aa22-158a>

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

8 June 2022 • 10:00 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com