Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

China-linked Hackers Exploit Cisco NX-OS as Zero-Day

Date of Publication	Admiralty Code	TA Number
July 2, 2024	A1	TA2024250

Summary

Exploited: April 2024
Affected Products: Cisco NX-OS Software
Impact: Cisco fixed a zero-day vulnerability in NX-OS that was exploited in assaults to install previously unidentified malware as root on susceptible switches. The vulnerability, identified as CVE-2024-20399, allows local attackers with Administrator capabilities to take control of the underlying operating systems of vulnerable devices and execute arbitrary commands with root permissions.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-20399	Cisco NX-OS Software CLI Command Injection Vulnerability	Cisco NX-OS Software	✓	✓	✓

Vulnerability Details

#1 A vulnerability in Cisco NX-OS software, identified as CVE-2024-20399, has been exploited by a China-linked hacking group. This flaw allows local attackers who already have Administrator privileges to gain control of vulnerable devices and execute commands with root-level permissions on the operating system.

#2 The flaw, CVE-2024-20399, results from inadequate validation of parameters provided to specific configuration CLI operations. Attackers can exploit this vulnerability by supplying specially crafted inputs to these commands. Successful exploitation grants them root access, allowing execution of arbitrary commands on the underlying operating system. Importantly, executed commands are not recorded in syslog, enabling attackers to bypass logging and stay undetected.

#3 To exploit this vulnerability, an attacker needs Administrator privileges on a Cisco NX-OS device. A cyber espionage group known as Velvet Ant, reportedly linked to China, has been seen using this zero-day vulnerability sine April to spread malware through Cisco NX-OS software, which is used in network switches. This specialized malware allows the group to upload more data, run code on the devices, and establish remote connections with infected Cisco Nexus devices.

#4 Given the active exploitation by sophisticated threat actors like Velvet Ant, it's crucial for administrators to be aware of this vulnerability and take necessary actions to secure their systems. This might include applying patches from Cisco, monitoring for unusual activity, and ensuring that only trusted administrators have access to the devices.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-20399	MDS 9000 Series Multilayer Switches Nexus 3000 Series Switches Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 6000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Switches in standalone NX-OS mode	cpe:2.3:h:cisco:nx-os:*:*:*:*:*:*:*	CWE-78

Recommendations

Update: Cisco has released a fixed version to mitigate the vulnerability (CVE-2024-20399). Users are strongly advised to update to this patched version promptly to safeguard their systems against potential exploitation.

Restrict Administrative Access: Regularly monitor and log all administrative activities and access. Isolate administrative systems and tools on a separate network segment to reduce the risk of attackers moving laterally.

SIEM Configuration: Integrating switch logs with a Security Information and Event Management (SIEM) system enhances the ability to correlate events and detect anomalies effectively.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1059.008 Network Device CLI	T1068 Exploitation for Privilege Escalation

Patch Details

To address the vulnerability (CVE-2024-20399), Cisco has released fixed version. It is strongly recommended that users update to the patched version immediately to protect their systems from potential exploitation.

Links:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP#fs

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

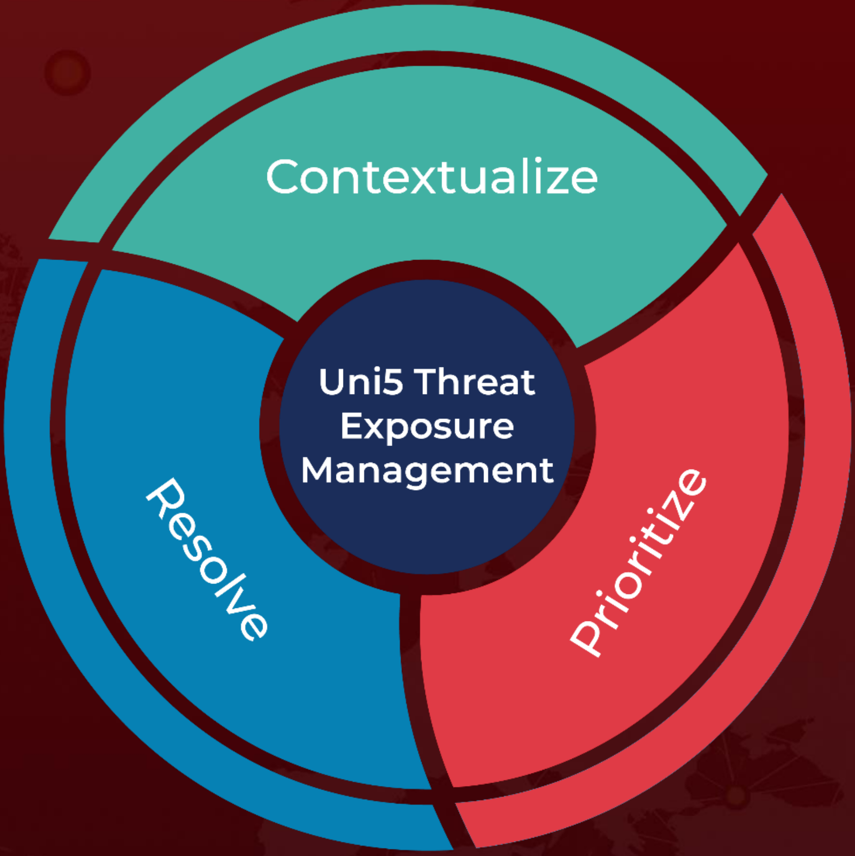
https://www.hivepro.com/threat-advisory/f5-big-ip-exploited-in-three-year-espionage-campaign-by-velvet-ant/

https://www.sygnia.co/threat-reports-and-advisories/china-nexus-threat-group-velvet-ant-exploits-cisco-0-day/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 2, 2024 • 7:00 AM

More at www.hivepro.com