مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Exploited Vulnerability in Cisco Switches

Tracking #:432316009

Date:03-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco released a security update to address a zero-day vulnerability in its switches, which has been actively exploited by attackers.

TECHNICAL DETAILS:

Cisco has patched an NX-OS zero-day exploited in April attacks to install previously unknown malware as root on vulnerable switches.

The threat actors gathered administrator-level credentials to gain access to Cisco Nexus switches and deploy a previously unknown custom malware that allowed them to remotely connect to compromised devices, upload additional files and execute malicious code.

Vulnerability Details:

- **CVE-2024-20399** | CVSS score: 6.0 - Medium | NX-OS Software CLI Command Injection Vulnerability
- This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands.
- An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command.
- A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.

Affected versions:

- 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

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected version to the fixed or latest versions released by Cisco.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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