CVE-2024-20397: Cisco NX-OS Software Image Verification Bypass Vulnerability

Vairav Advisory Report

Date: 2025-02-06

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A vulnerability CVE-2024-20397 has been identified in the bootloader of Cisco NX-OS Software. This vulnerability could allow an unauthenticated attacker with physical access to an affected device, or an authenticated local attacker with administrative credentials, to bypass NX-OS image signature verification that could lead to a malicious actor loading unverified software which provides a path for further escalation such as network-wide compromise.

VULNERABILITY DETAILS

CVE-2024-20397

- **Description:** The root cause of this vulnerability is due to insecure bootloader settings. This allows an attacker to execute a series of bootloader commands that allows them to bypass NX-OS image signature verification and load unverified software.
- **Impact:** If exploited, this vulnerability can lead to a series of further escalations such as installing malicious firmware, privilege escalation, persistent access, supply-chain attacks and even network-wide compromise.
- **CVSS Score:** 5.2 (Medium)

AFFECTED PRODUCTS

This vulnerability affects the following Cisco products if they are running a release of Cisco NX-OS Software that includes a vulnerable BIOS version, regardless of device configuration:

- MDS 9000 Series Multilayer Switches (CSCwh76163)
- Nexus 3000 Series Switches (CSCwm47438)
- Nexus 7000 Series Switches (CSCwh76166)
- Nexus 9000 Series Fabric Switches in ACI mode (CSCwn11901)
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCwm47438)
- UCS 6400 Series Fabric Interconnects (CSCwj35846)
- UCS 6500 Series Fabric Interconnects (CSCwj35846)

EXPLOIT DETAILS

This vulnerability can be exploited by the attacker executing a series of bootloader commands that will allow them to bypass NX-OS image signature verification.

RECOMMENDED ACTIONS

Patch & Upgrade*:*

- To the fixed BIOS versions for the affected products as released by Cisco for all affected switches in affected series.

ADDITIONAL SECURITY MEASURES

- Use Cisco's Trusted Image Verification (*show install verify*) to confirm image authenticity.
- Monitor logs and device integrity via Cisco SecureX, SIEM, or NX-OS syslogs for anomalies.
- Restrict access to firmware updates and harden administrative access (e.g., MFA, RBAC).

REFERENCES

- *https://app.opencve.io/cve/CVE-2024-20397*
- *https://www.cve.org/CVERecord?id=CVE-2024-20397*
- *https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL#fs*

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com