CVE-2025-20111: DENIAL OF SERVICE (DOS) VULNERABILITY

Vairav CVE News Report

Date: February 27, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Cisco has identified a high-severity vulnerability (CVE-2025-20111) affecting Cisco Nexus 3000 and 9000 Series Switches running NX-OS software in standalone mode. This vulnerability allows an unauthenticated, adjacent attacker to cause a denial-of-service (DoS) condition by sending a sustained rate of crafted Ethernet frames.

VULNERABILITY DETAILS

CVE-2025-20111: Layer 2 Ethernet Denial of Service Vulnerability

Description: This vulnerability stems from improper handling of specific Ethernet frames in the health monitoring diagnostics of Cisco Nexus switches. By sending a high rate of crafted Ethernet frames, an attacker can force an affected device to reload, causing an unexpected system to restart and disrupt network availability.

Impact: Service disruption, potential network instability.

CVSS Score: 7.4 (High)

AFFECTED VERSIONS

Cisco NX-OS Software:

- 9.3(1) to 9.3(14)
- 10.1(1) to 10.1(2t)
- 10.2(1) to 10.2(8)
- 10.3(1) to 10.3(5)
- 10.4(1) to 10.4(3)
- 10.5(1)

EXPLOIT DETAILS

Attackers can exploit this vulnerability remotely within an adjacent network. By continuously sending crafted Ethernet frames, they can overload the switch, forcing it to restart repeatedly. This can result in significant service disruptions, making it easier for attackers to execute further attacks by destabilizing network environments. No authentication is required for exploitation, increasing the risk to exposed devices.

RECOMMENDED ACTIONS

- Cisco recommends upgrading to the latest secure versions of NX-OS as soon as possible.
- Administrators should monitor Cisco's official advisory page for specific patch details and mitigation steps.

ADDITIONAL SECURITY MEASURES

- Implement rate limiting Layer 2 Ethernet traffic to reduce exposure to high-rate packet floods.
- Restrict access to management and critical networking interfaces to trusted segments.
- Enable logging and anomaly detection to identify unusual traffic patterns indicative of exploitation attempts.

REFERENCES

https://securityonline.info/cisco-warns-of-dos-vulnerability-in-nexus-3000-and-9000-series-switches-cve-2025-20111/

https://www.cve.org/CVERecord?id=CVE-2025-20111

https://nvd.nist.gov/vuln/detail/CVE-2025-20111

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: sales@vairavtech.com

Website: https://vairavtech.com