Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Cisco Nexus 3000 and 9000 Series Switches Intermediate System-to-Intermediate System Denial of Service Vulnerability

Vulnerability Note: VN-2025-21

Date of Issue: 29 August 2025

Severity Rating: High

Systems Affected:

This vulnerability affects the following Cisco products if they are running Cisco NX-OS Software, the IS-IS protocol is enabled, and the IS-IS protocol is enabled on at least one interface.

- Nexus 3000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

Description

A vulnerability has been identified in the Intermediate System-to-Intermediate System (IS-IS) feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload.

This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device. A successful exploit could allow the attacker to cause the unexpected restart of the IS-IS process, which could cause the affected device to reload, resulting in a denial of service (DoS) condition.

CVE Information
CVE-2025-20241

Workaround
Cisco has released software updates that address this vulnerability. More information is available on:

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n39k-isis-dos-JhJA8Rfx

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene