August 29, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Nexus 3000, 7000 and 9000 Series Switches running Cisco NX-OS Software

Technical Details

A vulnerability in the DHCPv6 relay agent of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to improper handling of specific fields in a DHCPv6 RELAY-REPLY message. An attacker could exploit this vulnerability by sending a crafted DHCPv6 packet to any IPv6 address that is configured on an affected device. A successful exploit could allow the attacker to cause the dhcp_snoop process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-20446 CVE-2024-20284 CVE-2024-20285 CVE-2024-20286 CVE-2024-20478 CVE-2024-20479 CVE-2023-38545 CVE-2024-20417
- Cisco Security Advisory – cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn
- Cisco Security Advisories