ESF LABS LIMITED

CYBER ADVISORY REPORT

CISCO NX-OS SOFTWARE DHCPV6 RELAY AGENT DOS VULNERABILITY | 8-30-2024

CYBER ADVISORY

EXECUTIVE SUMMARY

Cisco has patched a security vulnerability identified as **CVE-2024-20446** affecting the DHCPv6 relay agent of Cisco NX-OS software. This vulnerability could allow an unauthenticated, remote attacker to cause a denial-of-service (DoS) condition on an affected device.

This advisory report briefs the readers about the vulnerability and the recommendations that needed to apply in the organization as well as for the individuals to be protected from such threats. Further technical detailing has been mentioned in this report.

TECHNICAL DETAILS

The high severity vulnerability with details is mentioned below:

CVE ID	CVE-2024-20446
Vulnerability name	Cisco NX-OS Software DHCPv6 Relay Agent Denial of Service Vulnerability
CVSS score	8.6
Severity	High
Description	Cisco NX-OS Software is vulnerable to a denial of service, caused by improper handling of specific fields in a DHCPv6 RELAY-REPLY message. By sending a specially crafted DHCPv6 packet to any IPv6 address that is configured on an affected device, an attacker could exploit this vulnerability to cause the dhcp_snoop process to crash and restart multiple times.
Product(s) Affected	This vulnerability affects Cisco Nexus 3000 and 7000 Series Switches and Nexus 9000 Series Switches in standalone NX-OS mode if all the following conditions are true: • They are running Cisco NX-OS Software Release 8.2(11), 9.3(9), or 10.2(1). • They have the DHCPv6 relay agent enabled. • They have at least one IPv6 address configured on the device.
Exploitability	Remote, Unauthenticated
Impact	Network Interruption, Service Outage, and System Availability Loss
Recommendation(s)	• Cisco users are strongly recommended to apply the appropriate patches that affects Cisco NX-OS devices as soon as possible. • Users are advised to implement network segmentation to limit the potential impact of a successful attack. • It is advisable to maintain up-to-date software and firmware for all network devices to ensure timely application of security patches.

	• Users can determine the current remediation status or software version by using the Help function in the service GUI. • Users may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. • Users should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. • In case of urgency, users are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.
Reference(s)	• **https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn** • **https://nvd.nist.gov/vuln/detail/cve-2024-20446**