10 years CERT-EU

Security Advisory 2024-090

Multiple Vulnerabilities in Cisco NX-OS Software

2024-08-30 — v1.0

TLP:CLEAR

History:

- *30/08/2024 — v1.0 – Initial publication*

Summary

On August 28, Cisco released patches for multiple vulnerabilities affecting its NX-OS software, primarily used in Nexus switches. The most severe of these is a high-severity denial-of-service (DoS) vulnerability in the DHCPv6 relay agent, which could allow an unauthenticated remote attacker to cause targeted devices to reload repeatedly, leading to a DoS condition. Additionally, several medium-severity vulnerabilities were addressed, including issues that could allow privilege escalation and unauthorised code execution [1,2].

Technical Details

The vulnerability **CVE-2024-20446**, with a CVSS of 8.6, is due to improper handling of specific fields in DHCPv6 messages. By sending specially crafted DHCPv6 packets to an affected device, an attacker could cause the `dhcp_snoop` process to crash and restart multiple times, eventually forcing the device to reload, resulting in a DoS condition [3].

Other vulnerabilities addressed in this update include a medium-severity **Command Injection** flaw in the NX-OS CLI that could allow local attackers to execute arbitrary commands with elevated privileges, and multiple medium-severity **Privilege Escalation** flaws in the NX-OS sandbox environment that could allow authenticated local attackers to escape the Python sandbox and gain unauthorised access to the underlying operating system.

Affected Products

The vulnerability **CVE-2024-20446** 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 [3]:

- 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.

Recommendations

CERT-EU recommends applying the latest NX-OS patches provided by Cisco. Additionally, if DHCPv6 Relay Agent is not required in the environment, consider disabling this feature.

References

[1] https://www.securityweek.com/cisco-patches-multiple-nx-os-software-vulnerabilities/

[2] https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75417

[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn