مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Cisco

Tracking #:432316195

Date:29-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco released security updates to address a vulnerability in its NX-OS Software DHCPv6 Relay Agent.

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.

Vulnerability Details:

- **CVE-2024-20446 |** Base Score: 8.6 | Severity: High | Denial of Service Vulnerability
  - 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.

Affected Versions:

- 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, 9.3, or 10.2.
  - They have the DHCPv6 relay agent enabled.
  - They have at least one IPv6 address configured on the device.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Cisco.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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