مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Cisco NX-OS Software

Tracking #:432316592
Date:05-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Cisco NX-OS Software that could potentially be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-20397**
- Severity: High
- A vulnerability in the bootloader of Cisco NX-OS Software could allow an unauthenticated attacker with physical access or an authenticated local attacker with administrative credentials to bypass NX-OS image signature verification. This vulnerability is due to insecure bootloader settings and could potentially allow an attacker to load unverified software.
- The vulnerability exists in the bootloader of affected Cisco NX-OS Software versions. An attacker could exploit this vulnerability by executing a series of bootloader commands, potentially bypassing NX-OS image signature verification

Affected Products:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Switches (both ACI and standalone modes)
- UCS 6400 and 6500 Series Fabric Interconnects

Note: Refer to the Cisco advisory for mitigations and additional information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-image-sig-bypas-pQDRQvjL