مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Cisco IOS XR

Tracking #:432316051

Date:15-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco released security updates to address a vulnerability in Cisco IOS XR Software.

TECHNICAL DETAILS:

A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Cisco Secure Boot functionality and load unverified software on an affected device. To exploit this successfully, the attacker must have root-system privileges on the affected device.

Vulnerability Details:

- **CVE-2024-20456**- **Severity: High** -Cisco IOS XR Software Secure Boot Bypass Vulnerability
- This vulnerability is due to an error in the software build process. An attacker could exploit this vulnerability by manipulating the system's configuration options to bypass some of the integrity checks that are performed during the booting process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass of the requirement to run Cisco signed images or alter the security properties of the running system.

Affected versions:

Cisco IOS XR Release 24.2.1:

- 8000 Series Routers
- NCS 1010 Series Routers
- NCS 1014 Series Routers
- NCS 540 Series Routers that are running the NCS540L images
- NCS 5700 Fixed Port Series Routers, excluding NCS-57C3-MOD-S and NCS-57C3-MOD-SE-S

Fixed Version:

- Cisco IOS XR Release 24.2.11.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates 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-xr-secure-boot-quD5g8Ap