مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cisco Security Updates

Tracking #:432315663

Date:01-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco recently released security advisories to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On February 28, 2024, Cisco released security advisories addressing several vulnerabilities in multiple Cisco products. These include two high-severity flaws in NX-OS software. If exploited, these vulnerabilities could allow remote, unauthenticated attackers to gain unauthorized network access or launch denial-of-service (DoS) attacks on affected devices.

Vulnerabilities Details:

CVE	Severity	Description
CVE-2024-20321	High	Cisco NX-OS Software External Border Gateway Protocol Denial of Service Vulnerability
CVE-2024-20267	High	Cisco NX-OS Software MPLS Encapsulated IPv6 Denial of Service Vulnerability
CVE-2024-20344	Medium	Cisco UCS 6400 and 6500 Series Fabric Interconnects Intersight Managed Mode Denial of Service Vulnerability
CVE-2024-20291	Medium	Cisco Nexus 3000 and 9000 Series Switches Port Channel ACL Programming Vulnerability
CVE-2024-20294	Medium	Cisco FXOS and NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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/publicationListing.x