مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cisco Security Updates

Tracking #:432316218

Date:03-09-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Cisco released security advisories addressing several vulnerabilities in its NX-OS software and Application Policy Infrastructure Controller (APIC) products. These vulnerabilities could be exploited by attackers to gain unauthorized access, escalate privileges, or disrupt network operations.

Vulnerabilities Details:

Description	Severity	CVE
Cisco NX-OS Software DHCPv6 Relay Agent Denial of Service Vulnerability	High	CVE-2024-20446
Cisco NX-OS Software Python Sandbox Escape Vulnerabilities	Medium	CVE-2024-20284 CVE-2024-20285 CVE-2024-20286
Cisco NX-OS Software Command Injection Vulnerability	Medium	CVE-2024-20289
Cisco NX-OS Software Bash Arbitrary Code Execution and Privilege Escalation Vulnerabilities	Medium	CVE-2024-20411 CVE-2024-20413
Cisco Application Policy Infrastructure Controller Privilege Escalation Vulnerability	Medium	CVE-2024-20478
Cisco Application Policy Infrastructure Controller Unauthorized Policy Actions Vulnerability	Medium	CVE-2024-20279

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