مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cisco Security Updates

Tracking #:432316264

Date:12-09-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Cisco has released a security advisory addressing multiple vulnerabilities in its products. These vulnerabilities could potentially allow attackers to gain unauthorized access, execute malicious code, or disrupt network operations.

Vulnerabilities Details:

Description	Severity	CVE
Cisco Smart Licensing Utility Vulnerabilities	Critical	CVE-2024-20439 CVE-2024-20440
Cisco IOS XR Software UDP Packet Memory Exhaustion Vulnerability	High	CVE-2024-20304
Multiple Cisco Products Web-Based Management Interface Privilege Escalation Vulnerability	High	CVE-2024-20381
Cisco IOS XR Software Network Convergence System Denial of Service Vulnerability	High	CVE-2024-20317
Cisco IOS XR Software Segment Routing for Intermediate System-to-Intermediate System Denial of Service Vulnerability	High	CVE-2024-20406
Cisco IOS XR Software CLI Privilege Escalation Vulnerability	High	CVE-2024-20398
Cisco Routed Passive Optical Network Controller Vulnerabilities	High	CVE-2024-20483 CVE-2024-20489
Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion): July 2024	High	CVE-2024-6387
Cisco Meraki Systems Manager Agent for Windows Privilege Escalation Vulnerability	High	CVE-2024-20430
RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024	High	CVE-2024-3596
Cisco IOS XR Software Dedicated XML Agent TCP Denial of Service Vulnerability	Medium	CVE-2024-20390
Cisco IOS XR Software CLI Arbitrary File Read Vulnerability	Medium	CVE-2024-20343
Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability	Medium	CVE-2024-20466
Cisco Identity Services Engine Command Injection Vulnerability	Medium	CVE-2024-20469
Cisco Expressway Edge Improper Authorization Vulnerability	Medium	CVE-2024-20497
Cisco Duo Epic for Hyperdrive Information Disclosure Vulnerability	Medium	CVE-2024-20503
Multiple Cisco Products OpenSocial Gadget Editor Vulnerabilities	Medium	CVE-2021-1245 CVE-2021-1246

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