مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432317647

Date:28-08-2025

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Cisco has released security updates to address multiple vulnerabilities affecting a wide range of its products, including Cisco IOS, IOS XE, NX-OS, UCS Manager, Secure Firewall, and other Cisco solutions. Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, conduct denial-of-service (DoS) attacks, perform cross-site scripting (XSS), bypass security restrictions, or gain unauthorized access to sensitive information.

Critical Vulnerability

- **CVE-2018-0171** – Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability

High-Severity Vulnerabilities

- **CVE-2025-20317** – Cisco Integrated Management Controller Virtual Keyboard Video Monitor Open Redirect Vulnerability
- **CVE-2025-20241** – Cisco Nexus 3000 and 9000 Series Switches Intermediate System-to-Intermediate System Denial of Service Vulnerability
- **CVE-2025-20134** – Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SSL/TLS Certificate Denial of Service Vulnerability

Medium-Severity Vulnerabilities

- **CVE-2025-20296** – Cisco UCS Manager Software Stored Cross-Site Scripting Vulnerability
- **CVE-2025-20294, CVE-2025-20295** – Cisco UCS Manager Software Command Injection Vulnerabilities
- **CVE-2025-20342** – Cisco Integrated Management Controller Virtual Keyboard Video Monitor Stored Cross-Site Scripting Vulnerability
- **CVE-2025-20262** – Cisco Nexus 3000 and 9000 Series Switches Protocol Independent Multicast Version 6 Denial of Service Vulnerability
- **CVE-2025-20290** – Cisco NX-OS Software Sensitive Log Information Disclosure Vulnerability
- **CVE-2025-20292** – Cisco NX-OS Software Command Injection Vulnerability
- **CVE-2025-20347, CVE-2025-20348** – Cisco Nexus Dashboard and Nexus Dashboard Fabric Controller Unauthorized REST API Vulnerabilities
- **CVE-2025-20344** – Cisco Nexus Dashboard Path Traversal Vulnerability
- **CVE-2025-20131** – Cisco Identity Services Engine Arbitrary File Upload Vulnerability
- **CVE-2025-20269** – Cisco Evolved Programmable Network Manager and Cisco Prime Infrastructure Sensitive Information Disclosure Vulnerability
- **CVE-2025-20345** – Cisco Duo Authentication Proxy Information Disclosure 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