مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432318727

Date:06-04-2026

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 addressing multiple vulnerabilities across its enterprise networking and management products. These vulnerabilities include improper authorization, privilege escalation, remote code execution (RCE), denial of service (DoS), and web-based attacks. Successful exploitation could allow attackers to gain elevated privileges, execute arbitrary commands, disrupt services, or access sensitive data.

High Severity Vulnerabilities

- Cisco Evolved Programmable Network Manager Improper Authorization Vulnerability – CVE-2026-20155
- Cisco Smart Software Manager On-Prem Privilege Escalation Vulnerability – CVE-2026-20151
- Cisco Integrated Management Controller Command Injection and Remote Code Execution Vulnerabilities – CVE-2026-20094, CVE-2026-20095, CVE-2026-20096

Medium Severity Vulnerabilities

- Cisco IOS XE Software Denial of Service Vulnerability – CVE-2026-20110
- Cisco Nexus Dashboard Insights Arbitrary File Write Vulnerability – CVE-2026-20174
- Cisco Nexus Dashboard and Nexus Dashboard Insights Server-Side Request Forgery Vulnerability – CVE-2026-20041
- Cisco Nexus Dashboard Configuration Backup REST API Unauthorized Access Vulnerability – CVE-2026-20042
- Cisco Integrated Management Controller Cross-Site Scripting Vulnerabilities – CVE-2026-20085, CVE-2026-20087, CVE-2026-20088

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