مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432318910

Date:07-05-2026

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 affecting several Cisco products, including Cisco Unity Connection, Cisco Identity Services Engine (ISE), Cisco SG350/SG350X Switches, Cisco Prime Infrastructure, Cisco Crosswork Network Controller, Cisco IoT Field Network Director, Cisco Slido, and Cisco Enterprise Chat and Email.

Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, bypass authentication, conduct denial of service (DoS) attacks, upload malicious files, disclose sensitive information, or perform cross-site scripting (XSS) attacks.

Vulnerability Details

High Severity

- **CVE-2026-20034, CVE-2026-20035** – Cisco Unity Connection Remote Code Execution and Server-Side Request Forgery Vulnerabilities
- **CVE-2026-20185** – Cisco SG350 and SG350X Series Managed Switches SNMP Denial of Service Vulnerability
- **CVE-2026-20188** – Cisco Crosswork Network Controller and Cisco Network Services Orchestrator Connection Exhaustion Denial of Service Vulnerability
- **CVE-2026-20167, CVE-2026-20168, CVE-2026-20169** – Cisco IoT Field Network Director Vulnerabilities

Medium Severity

- **CVE-2026-20219** – Cisco Slido Insecure Direct Object Reference Vulnerability
- **CVE-2026-20189** – Cisco Prime Infrastructure Information Disclosure Vulnerability
- **CVE-2026-20193, CVE-2026-20195** – Cisco Identity Services Engine Authentication Bypass Vulnerabilities
- **CVE-2026-20172** – Cisco Enterprise Chat and Email Lite Agent File Upload Vulnerability
- **CVE-2025-20204, CVE-2025-20205** – Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities

Note

Refer to the official Cisco security advisory for detailed information regarding affected products, impacted software versions, fixed releases, and recommended mitigation measures.

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