مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432319153

Date:18-06-2026

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 to address multiple vulnerabilities affecting several products, including Cisco Identity Services Engine (ISE), Cisco Catalyst SD-WAN Controller, Cisco Webex App, Cisco Umbrella Virtual Appliance, and Cisco Crosswork Network Controller. The vulnerabilities range from medium to critical severity and could allow remote code execution, authentication bypass, privilege escalation, information disclosure, open redirect attacks, and server-side template injection.

Vulnerability Details

Critical Severity

- **CVE-2026-20181 – Cisco ISE Remote Code Execution Vulnerability**
  Could allow an unauthenticated attacker to execute arbitrary code on an affected system.
- **CVE-2026-20190 – Cisco ISE Information Disclosure Vulnerability**
  Could allow unauthorized access to sensitive information.
- **CVE-2026-20127 – Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability**
  Could allow an unauthenticated attacker to bypass authentication and gain unauthorized access.
- **CVE-2026-20182 – Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability**
  Could allow attackers to circumvent authentication controls and perform unauthorized actions.

Medium Severity

- **CVE-2026-20178 – Cisco Webex App Open Redirect Vulnerability**
  Could allow attackers to redirect users to malicious websites.
- **CVE-2026-20246 – Cisco Umbrella Virtual Appliance Privilege Escalation Vulnerability**
  Could allow a local authenticated attacker to obtain elevated privileges.
- **CVE-2026-20220 – Cisco Crosswork Network Controller Server-Side Template Injection Vulnerability**
  Could allow an authenticated attacker to execute unauthorized commands.

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