مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

# Security Updates - Cisco

Tracking #:432318567

Date:11-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

## 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 Cisco IOS XR Software and Cisco Contact Center products. These vulnerabilities could allow attackers to cause denial-of-service (DoS) conditions, escalate privileges, or execute cross-site scripting (XSS) attacks in affected environments.

**Vulnerability Details**

- **CVE-2026-20118 – Cisco IOS XR Egress Packet Network Interface Aligner Interrupt Denial of Service Vulnerability**
  - **Severity:** High
  - A vulnerability in Cisco IOS XR Software could allow specially crafted traffic to cause a denial-of-service condition on affected devices.
- **CVE-2026-20074 – Cisco IOS XR Software Multi-Instance IS-IS Denial of Service Vulnerability**
  - **Severity:** High
  - A flaw in the Multi-Instance IS-IS feature of Cisco IOS XR Software could allow crafted protocol traffic to cause a denial-of-service condition.
- **CVE-2026-20040 & CVE-2026-20046 – Cisco IOS XR Software CLI Privilege Escalation Vulnerabilities**
  - **Severity:** High
  - These vulnerabilities could allow a locally authenticated user to escalate privileges through the command-line interface.
- **CVE-2026-20116 & CVE-2026-20117 – Cisco Contact Center Products Cross-Site Scripting Vulnerabilities**
  - **Severity:** Medium
  - These vulnerabilities could allow malicious scripts to be injected into a web interface and executed in a user's browser.

## 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