مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432318356

Date:05-02-2026

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 TelePresence and RoomOS Software, Cisco Meeting Management, Cisco Secure Web Appliance, Cisco Prime Infrastructure, and Cisco Evolved Programmable Network Manager (EPNM).
These vulnerabilities range from Denial of Service (DoS) and Arbitrary File Upload to Cross-Site Scripting (XSS) and Open Redirect, potentially allowing attackers to disrupt services, upload malicious files, or perform client-side attacks.

Vulnerability Details

1. Cisco TelePresence Collaboration Endpoint Software and RoomOS – Denial of Service

- **CVE ID:** CVE-2026-20119
- **Severity:** High
- A vulnerability exists in Cisco TelePresence Collaboration Endpoint Software and RoomOS due to improper handling of crafted network requests. An unauthenticated remote attacker could exploit this vulnerability to trigger a Denial of Service (DoS) condition, causing the affected device to become unresponsive and requiring a manual restart to recover.

2. Cisco Meeting Management – Arbitrary File Upload

- **CVE ID:** CVE-2026-20098
- **Severity:** High
- Cisco Meeting Management contains an arbitrary file upload vulnerability caused by insufficient validation of uploaded files. An authenticated attacker could exploit this vulnerability to upload malicious files to the server, potentially leading to remote code execution, system compromise, or unauthorized access to sensitive data.

3. Cisco Secure Web Appliance – Real-Time Scanning Archive File Bypass

- **CVE ID:** CVE-2026-20056
- **Severity:** Medium
- A vulnerability in Cisco Secure Web Appliance allows specially crafted archive files to bypass real-time malware scanning. An attacker could exploit this issue to deliver malicious content that is not properly inspected, increasing the risk of malware infections within the organization.

4. Cisco Prime Infrastructure – Stored Cross-Site Scripting (XSS)

- **CVE ID:** CVE-2026-20111
- **Severity:** Medium
- A vulnerability in the Cisco Prime Infrastructure web-based management interface could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack. The issue is caused by insufficient validation of user-supplied input, allowing an attacker with administrative credentials to inject malicious script code that may execute in users' browsers and expose sensitive, browser-based information.

5. Cisco Evolved Programmable Network Manager and Cisco Prime Infrastructure – Open Redirect

- **CVE ID:** CVE-2026-20123
- **Severity:** Medium
- A vulnerability in the web-based management interfaces of Cisco EPNM and Cisco Prime

Infrastructure could allow an unauthenticated, remote attacker to redirect users to a malicious web page due to improper input validation in HTTP request parameters.

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