

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Cisco**

Tracking #:432316727

Date:10-01-2025

## 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 Common Services Platform Collector (CSPC), Cisco Crosswork Network Controller, and Cisco ThousandEyes Agent. These vulnerabilities could allow authenticated attackers to conduct cross-site scripting (XSS) attacks or intercept metrics information.

### Vulnerabilities Details:

#### Cisco Common Services Platform Collector Cross-Site Scripting Vulnerabilities

- **CVE IDs:** CVE-2025-20166, CVE-2025-20167, CVE-2025-20168
- **CVSS Base Score:** 5.4 (Medium)
- **Impact:** An authenticated, remote attacker could conduct XSS attacks against users of the web-based management interface.
- **Details:** Insufficient validation of user-supplied input allows injection of malicious code into specific interface pages.

#### Cisco Crosswork Network Controller Stored Cross-Site Scripting Vulnerabilities

- **CVE ID:** CVE-2025-20123
- **CVSS Base Score:** 4.8 (Medium)
- **Impact:** An authenticated, remote attacker with valid administrative credentials could conduct XSS attacks against users of the web-based management interface.
- **Details:** Improper validation of user-supplied input in specific data fields of the interface.

#### Cisco ThousandEyes Agent Certificate Validation Vulnerability

- **CVE ID:** CVE-2025-20126
- **CVSS Base Score:** 4.8 (Medium)
- **Impact:** An unauthenticated, remote attacker could intercept or manipulate metrics information.
- **Details:** Improper validation of certificates for hosted metrics services allows potential on-path attacks using crafted certificates.

### Affected Products:

- Cisco Common Services Platform Collector (CSPC)
- Cisco Crosswork Network Controller
- Cisco ThousandEyes Endpoint Agent for macOS and RoomOS

## 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/content/CiscoSecurityAdvisory/cisco-sa-cspc-xss-CDOJZyH>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xwork-xss-KCcg7WwU>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thousandeyes-cert-pqtJUv9N>