مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates - Cisco

Tracking #:432317824

Date:16-10-2025

## 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 across several of its products, including Desk Phones, IP Phones, Video Phones, IOS XE Software, Snort 3, and TelePresence Collaboration systems. Exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, bypass secure boot protections, cause denial of service, or gain unauthorized access to sensitive information.

**Vulnerability Details:**

**1. Cisco Desk Phone 9800 Series, IP Phone 7800 and 8800 Series, and Video Phone 8875 with SIP Software Vulnerabilities**

- **Severity:** High
- **CVE IDs:** CVE-2025-20350, CVE-2025-20351
- **Description:** Multiple vulnerabilities in the Session Initiation Protocol (SIP) software of Cisco Desk Phone and IP Phone products could allow an unauthenticated, remote attacker to cause a denial of service (DoS) or potentially execute arbitrary code.

**2. Cisco IOS XE Software Secure Boot Bypass Vulnerabilities**

- **Severity:** High
- **CVE IDs:** CVE-2025-20313, CVE-2025-20314
- **Description:** Multiple vulnerabilities in the Secure Boot implementation of Cisco IOS XE Software could allow a local attacker with root privileges to bypass secure boot restrictions, potentially leading to the loading of unauthorized software or system compromise.

**3. Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities**

- **Severity:** Medium
- **CVE IDs:** CVE-2025-20359, CVE-2025-20360
- **Description:** Multiple denial-of-service (DoS) vulnerabilities exist in the Snort 3 detection engine's handling of MIME data. An attacker could exploit these vulnerabilities by sending specially crafted traffic to cause the Snort 3 process to restart unexpectedly.

**4. Cisco TelePresence Collaboration Endpoint and RoomOS Software Information Disclosure Vulnerability**

- **Severity:** Medium
- **CVE ID:** CVE-2025-20329
- **Description:** A vulnerability in Cisco TelePresence and RoomOS Software could allow an authenticated, remote attacker to access sensitive information due to improper access control.

## 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