مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates - Cisco

Tracking #:432317967

Date:07-11-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Cisco has released security updates to address multiple vulnerabilities affecting several Cisco products. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, gain unauthorized access, cause a denial of service, or disclose sensitive information.

## TECHNICAL DETAILS:

**Vulnerability Details:**
**Critical-Severity Vulnerabilities**

- **CVE-2025-20333** — Cisco ASA & FTD VPN Web Server Remote Code Execution
  - Allows remote attackers to execute arbitrary code via crafted requests to the VPN web interface.
- **CVE-2025-20363** — Cisco ASA, FTD, IOS, IOS XE & IOS XR Web Services Remote Code Execution
  - Unauthenticated attackers could run arbitrary commands on vulnerable devices through web services.
- **CVE-2025-20354 / CVE-2025-20358** — Cisco Unified Contact Center Express Remote Code Execution
  - Could lead to full system compromise if exploited.

**High-Severity Vulnerability**

- **CVE-2025-20343** — Cisco ISE RADIUS Suppression Denial of Service
  - May allow attackers to disrupt network authentication services, causing denial of service.

**Medium-Severity Vulnerabilities**

- **CVE-2025-20362** — Cisco ASA & FTD VPN Web Server Unauthorized Access
  - Unauthorized users may access restricted VPN web services.
- **CVE-2025-20289 / 20303 / 20304** — Cisco ISE Reflected XSS & Information Disclosure
  - Could allow attackers to inject scripts or view sensitive information via the web interface.
- **CVE-2025-20374 / 20375 / 20376** — Multiple Cisco Contact Center Products
  - May allow limited unauthorized actions or information disclosure.
- **CVE-2025-20307** — Cisco BroadWorks CommPilot XSS
  - Cross-site scripting vulnerability could execute malicious scripts in users' browsers.

**Impact**
Successful exploitation of this vulnerabilities could lead to remote code execution, unauthorized access, denial of service, or information disclosure, potentially allowing full system compromise or data leakage.

## 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