مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432317691

Date:11-09-2025

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 advisories addressing several high and medium severity vulnerabilities affecting IOS XR platforms and Secure Firewall appliances. Successful exploitation can lead to denial of service, security control bypass, and malicious software installation. Immediate remediation actions are recommended to mitigate potential risks.

Vulnerabilities Details:

1. Cisco IOS XR Software Image Verification Bypass Vulnerability

- **CVE ID:** CVE-2025-20248
- **Severity:** High
- **Description:** A vulnerability in Cisco IOS XR Software could allow an attacker to bypass image verification checks. An attacker with access to a vulnerable system could install malicious or tampered images, leading to unauthorized code execution and persistent compromise.
- **Impact:** Unauthorized software execution, potential system compromise.

2. Cisco IOS XR ARP Broadcast Storm Denial of Service Vulnerability

- **CVE ID:** CVE-2025-20340
- **Severity:** High
- **Description:** A vulnerability in ARP packet handling of Cisco IOS XR could allow an attacker to trigger a broadcast storm. This may result in high CPU utilization and denial of service (DoS).
- **Impact:** Service disruption, routing instability, DoS condition.

3. Cisco IOS XR Software Management Interface ACL Bypass Vulnerability

- **CVE ID:** CVE-2025-20159
- **Severity:** Medium
- **Description:** A vulnerability in the access control logic of Cisco IOS XR management interfaces may allow an attacker to bypass ACLs. This could result in unauthorized access to management services.
- **Impact:** Unauthorized management access, increased attack surface.

4. Cisco Secure Firewall ASA & FTD IPv6 over IPsec Denial of Service Vulnerability

- **CVE ID:** CVE-2025-20222
- **Severity:** High
- **Description:** A vulnerability in IPv6 over IPsec processing for Cisco Secure Firewall Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software for Firepower 2100 Series may allow an attacker to cause a DoS condition by sending crafted traffic.
- **Impact:** DoS leading to service disruption and loss of availability.

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