مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Cisco

Tracking #:432318661

Date:26-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

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 multiple security advisories addressing several high-severity and one critical vulnerability impacting widely deployed networking and security products, including IOS, IOS XE, ASA, Secure Firewall Threat Defense (FTD), and FMC.

Technical Details

1. **Critical Remote Code Execution (FMC)**
   - **CVE:** CVE-2026-20131
   - **Affected Products:** Cisco Secure Firewall Management Center
   - **CVSS Score:** 10.0 (Critical)
   - **CWE:** CWE-502 (Deserialization of Untrusted Data)
   - **Advisory ID:** cisco-sa-fmc-rce-NKhnULJh

2. **IKEv2 Denial of Service Vulnerability**
   - **CVE:** CVE-2026-20012
   - **Affected Products:** Cisco IOS, IOS XE, ASA, Secure Firewall FTD
   - **CVSS Score:** 8.6 (High)
   - **CWE:** CWE-401 (Memory Leak)
   - **Advisory ID:** cisco-sa-asa-ftd-ios-dos-kPEpQGGK

3. **DHCP Snooping DoS Vulnerability (Catalyst 9000)**
   - **CVE:** CVE-2026-20084
   - **Affected Products:** Cisco IOS XE (Catalyst 9000 Series)
   - **CVSS Score:** 8.6 (High)
   - **CWE:** CWE-400 (Resource Consumption)
   - **Advisory ID:** cisco-sa-bootp-WuBhNBxA

4. **HTTP Server DoS Vulnerability**
   - **CVE:** CVE-2026-20125
   - **Affected Products:** Cisco IOS / IOS XE Release 3E
   - **CVSS Score:** 7.7 (High)
   - **CWE:** CWE-228
   - **Advisory ID:** cisco-sa-ios-http-dos-sbv8XRpL

5. **TLS Memory Exhaustion DoS**
   - **CVE:** CVE-2026-20004
   - **Affected Products:** Cisco IOS XE
   - **CVSS Score:** 7.4 (High)
   - **CWE:** CWE-771 (Missing Resource Release)
   - **Advisory ID:** cisco-sa-iosxe-tls-dos-TVgLDEZL

6. **CAPWAP DoS (Wireless Controllers)**
   - **CVE:** CVE-2026-20086
   - **Affected Products:** Catalyst CW9800 Wireless Controllers
   - **CVSS Score:** 8.6 (High)
   - **CWE:** CWE-230
   - **Advisory ID:** cisco-sa-wlc-dos-hnX5KGOm

7. **Secure Boot Bypass Vulnerability**
   - **CVE:** CVE-2026-20104
   - **Affected Products:** Cisco Catalyst & Rugged Series Switches
   - **CVSS Score:** 6.1 (Medium)
   - **CWE:** CWE-124
   - **Advisory ID:** cisco-sa-xe-secureboot-bypass-B6uYxYSZ

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-asa-ftd-ios-dos-kPEpQGGK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bootp-WuBhNBxA
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-http-dos-sbv8XRpL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-tls-dos-TVgLDEZL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-hnX5KGOm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-secureboot-bypass-B6uYxYSZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh