مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432318517

Date:05-03-2026

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 addressing multiple vulnerabilities affecting several Cisco products. These vulnerabilities range from Critical to Medium severity and could allow attackers to cause denial-of-service (DoS), execute arbitrary commands, bypass security controls, or perform unauthorized access.

Vulnerabilities Details

Critical Severity

- Cisco Catalyst SD-WAN Vulnerabilities – CVE-2026-20122, CVE-2026-20126, CVE-2026-20128

High Severity

- Cisco Secure Firewall Management Center Software SQL Injection Vulnerabilities – CVE-2026-20001, CVE-2026-20002, CVE-2026-20003
- Cisco Secure Firewall ASA & Secure Firewall Threat Defense Remote Access SSL VPN DoS Vulnerabilities – CVE-2026-20100, CVE-2026-20101, CVE-2026-20103
- Cisco Secure Firewall ASA & Secure Firewall Threat Defense VPN Web Server DoS Vulnerability – CVE-2026-20039
- Cisco Secure Firewall ASA & Secure Firewall Threat Defense IKEv2 DoS Vulnerabilities – CVE-2026-20013, CVE-2026-20014, CVE-2026-20015
- Cisco Secure Firewall ASA & Secure Firewall Threat Defense IPsec DoS Vulnerability – CVE-2026-20049
- Cisco Secure Firewall ASA Multiple Context Mode SCP Unauthorized File Access Vulnerability – CVE-2026-20062
- Cisco Secure Firewall ASA TCP Flood DoS Vulnerability – CVE-2026-20082

Medium Severity

- Cisco Secure Firewall Management Center SQL Injection Vulnerability – CVE-2024-20340
- Cisco ASA & Firepower Threat Defense Command Injection Vulnerability – CVE-2024-20358
- Cisco Webex Services Cross-Site Scripting Vulnerability – CVE-2026-20149
- Multiple Cisco Products Snort 3 DoS Vulnerabilities – CVE-2026-20005, CVE-2026-20065, CVE-2026-20066
- Cisco Secure Firewall Management Center & Threat Defense Path Traversal Vulnerability – CVE-2026-20018
- Cisco Secure Firewall Threat Defense TLS with Snort 3 Detection Engine DoS Vulnerability – CVE-2026-20006
- Cisco Secure Firewall Threat Defense Snort 3 SSL Memory Management DoS Vulnerability – CVE-2026-20052
- Multiple Cisco Products Snort 3 VBA DoS Vulnerabilities – CVE-2026-20053, CVE-2026-20054, CVE-2026-20057
- Cisco Secure Firewall Threat Defense Snort Deep Inspection Bypass Vulnerability – CVE-2026-20007
- Cisco Secure Firewall Threat Defense SSL Decryption Policy DoS Vulnerability – CVE-2026-20050

- Cisco ASA & Secure Firewall Threat Defense Authenticated Command Injection Vulnerabilities – CVE-2026-20016, CVE-2026-20017, CVE-2026-20063
- Cisco Secure Firewall Management Center Command Injection Vulnerability – CVE-2026-20044
- ClamAV CSS Image Parsing Error Handling DoS Vulnerability – CVE-2026-20031
- Cisco ASA & Secure Firewall Threat Defense VPN Web Services Cross-Site Scripting Vulnerability – CVE-2026-20070
- Cisco ASA & Secure Firewall Threat Defense SAML Reflected Cross-Site Scripting Vulnerability – CVE-2026-20102
- Cisco ASA & Secure Firewall Threat Defense OSPF Protocol Vulnerabilities – CVE-2026-20020, CVE-2026-20021, CVE-2026-20022
- Cisco ASA & Secure Firewall Threat Defense Lua Code Injection Vulnerability – CVE-2026-20008
- Cisco ASA & Secure Firewall Threat Defense VPN Web Services Client-Side Request Smuggling Vulnerability – CVE-2026-20069
- Cisco ASA & Secure Firewall Threat Defense Access Control List Bypass Vulnerability – CVE-2026-20073
- Cisco ASA SSH Partial Private Key Authentication Bypass Vulnerability – CVE-2026-20009

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