مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Cisco

Tracking #:432317607

Date:15-08-2025

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 affecting various Cisco products, including Cisco Secure Firewall Management Center Software, Secure Firewall Threat Defense Software, Adaptive Security Appliance (ASA), IOS, and IOS XE. Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, cause denial-of-service (DoS) conditions, or perform malicious actions that could disrupt network security operations.

Critical Severity Vulnerabilities

- Cisco Secure Firewall Management Center Software – RADIUS Remote Code Execution Vulnerability – CVE-2025-20265

High Severity Vulnerabilities

- Cisco Secure Firewall Threat Defense Software – Snort 3 Denial of Service Vulnerability – CVE-2025-20217
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Firepower 2100 Series – IPv6 over IPsec Denial of Service Vulnerability – CVE-2025-20222
- Cisco Secure Firewall Management Center Software – HTML Injection Vulnerability – CVE-2025-20148
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software – Remote Access VPN Web Server Denial of Service Vulnerability – CVE-2025-20244
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software – Remote Access SSL VPN Denial of Service Vulnerabilities – CVE-2025-20133, CVE-2025-20243
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software – SSL/TLS Certificate Denial of Service Vulnerability – CVE-2025-20134
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software – Network Address Translation DNS Inspection Denial of Service Vulnerability – CVE-2025-20136
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software – VPN Web Server Denial of Service Vulnerability – CVE-2025-20251
- Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software – IKEv2 Denial of Service Vulnerabilities – CVE-2025-20224, CVE-2025-20225, CVE-2025-20239
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software – Web Services Denial of Service Vulnerability – CVE-2025-20263
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Firepower 3100 and 4200 Series – TLS 1.3 Cipher Denial of Service Vulnerability – CVE-2025-20127

Impact

- Critical risk: Remote Code Execution (CVE-2025-20265) could allow a remote, unauthenticated attacker to execute arbitrary code with elevated privileges.
- High risk: Multiple Denial-of-Service vulnerabilities could allow attackers to disrupt device availability, impact VPN services, terminate secure connections, and degrade overall firewall performance.
- Successful exploitation may lead to network downtime, security policy bypass, and loss of availability for critical services.

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?product=Cisco&sort=-day_sir#~Vulnerabilities