مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Cisco Products

Tracking #:432317232

Date:08-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco released security advisories addressing multiple critical and high-severity vulnerabilities impacting a broad range of its products, including Cisco IOS XE, IOS, IOS XR, Wireless Controllers, SD-WAN Manager, Catalyst switches, and security appliances.

TECHNICAL DETAILS:

Cisco released security advisories addressing multiple critical and high-severity vulnerabilities impacting a broad range of its products, including Cisco IOS XE, IOS, IOS XR, Wireless Controllers, SD-WAN Manager, Catalyst switches, and security appliances. These vulnerabilities span across **unauthenticated remote code execution (RCE)**, **arbitrary file uploads**, **privilege escalation**, and **denial-of-service (DoS)** attacks. The most severe, **CVE-2025-32433**, allows **unauthenticated RCE in Erlang/OTP SSH Server** used in multiple Cisco products. Immediate remediation is strongly recommended to prevent exploitation.

Critical Vulnerabilities

CVE	Description	CVSS	Affected Products
CVE-2025-32433	Unauthenticated Remote Code Execution in Erlang/OTP SSH Server	10.0	Multiple Cisco Products using Erlang/OTP
CVE-2025-20188	Arbitrary File Upload in Cisco IOS XE Wireless Controller Software	10.0	IOS XE Wireless Controllers

High Severity Vulnerabilities:

- CVE-2025-20140: Cisco IOS XE Software for WLC Wireless IPv6 Clients Denial of Service Vulnerability
- CVE-2025-20186: Cisco IOS XE Software Web-Based Management Interface Command Injection Vulnerability
- CVE-2025-20154: Cisco IOS, IOS XE, and IOS XR Software TWAMP Denial of Service Vulnerability
- CVE-2025-20191: Multiple Cisco Products Switch Integrated Security Features DHCPv6 Denial of Service Vulnerability
- CVE-2025-20122: Cisco Catalyst SD-WAN Manager Privilege Escalation Vulnerability
- CVE-2025-20182: Cisco Adaptive Security Appliance Software, Firepower Threat Defense Software, IOS Software, and IOS XE Software IKEv2 Denial of Service Vulnerability
- CVE-2025-20197: Cisco IOS XE Software Privilege Escalation Vulnerability
- CVE-2025-20198: Cisco IOS XE Software Privilege Escalation Vulnerability
- CVE-2025-20192: Cisco IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability
- CVE-2025-20162: Cisco IOS XE Software DHCP Snooping Denial of Service Vulnerability
- CVE-2025-20164: Cisco IOS Software Industrial Ethernet Switch Device Manager Privilege Escalation Vulnerability
- CVE-2025-20202: Cisco IOS XE Wireless Controller Software Cisco Discovery Protocol

Denial of Service Vulnerability

- CVE-2025-20210: Cisco Catalyst Center Unauthenticated API Access Vulnerability
- CVE-2025-20181: Cisco IOS Software for Cisco Catalyst 2960X, 2960XR, 2960CX, and 3560CX Series Switches Secure Boot Bypass Vulnerability
- CVE-2025-20189: Cisco IOS XE Software for Cisco ASR 903 Aggregation Services Routers ARP Denial of Service Vulnerability

RECOMMENDATIONS:

- Prioritize patching CVE-2025-32433 and CVE-2025-20188 due to their unauthenticated and remotely exploitable nature.
- Apply Cisco-provided security updates or interim mitigations available via Cisco Security Advisories.

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