مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Cisco SNMP

Tracking #:432317750

Date:25-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has issued a security advisory for an actively exploited SNMP subsystem vulnerability affecting Cisco IOS and IOS XE Software.

TECHNICAL DETAILS:

Cisco has issued a security advisory for a critical SNMP subsystem vulnerability (CVE-2025-20352) affecting Cisco IOS and IOS XE Software. This flaw is actively exploited in the wild and can allow attackers with SNMP credentials to achieve denial of service (DoS) or remote code execution (RCE) as root, leading to full system compromise.

The vulnerability stems from a stack overflow condition triggered by specially crafted SNMP packets. Exploitation has already been observed in real-world attacks, particularly after administrator credentials were compromised.

Given the active exploitation and potential for complete takeover of affected devices, immediate patching and mitigations are strongly recommended.

Vulnerability Details:

- CVE: CVE-2025-20352
- CWE: CWE-121 (Stack-based Buffer Overflow)
- CVSS v3.1 Score: 7.7 (High)
- Attack Vector: Remote, via IPv4/IPv6
- Privileges Required: Low (for DoS), High (for RCE as root)
- Impact:
- DoS: Reload of affected devices
- RCE: Arbitrary code execution as root
- Affected Products:
  - Cisco IOS Software
  - Cisco IOS XE Software
  - Meraki MS390 and Catalyst 9300 running Meraki CS 17 or earlier
- Fixed Version: Cisco IOS XE Software Release 17.15.4a or later.
- Exploitation Status: Confirmed active exploitation in the wild.
- Mitigation: Exclude affected OIDs by configuring SNMP views to block malicious queries

The September 24, 2025, release of the Cisco IOS and IOS XE Software Security Advisory Bundled Publication includes 13 Cisco Security Advisories that describe 14 vulnerabilities in Cisco IOS Software and Cisco IOS XE Software. Cisco has released software updates that address these vulnerabilities.

Other Vulnerabilities:

Cisco IOS XE Software HTTP API Command Injection Vulnerability	CVE-2025-20334	High	8.8
Cisco IOS XE Software Network-Based Application Recognition Denial of Service Vulnerability	CVE-2025-20315	High	8.6

Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability	CVE-2025-20160	High	8.1
Cisco IOS Software Industrial Ethernet Switch Device Manager Denial of Service Vulnerability	CVE-2025-20327	High	7.7
Cisco IOS XE Software Simple Network Management Protocol Denial of Service Vulnerability	CVE-2025-20312	High	7.7
Cisco IOS XE Software for Catalyst 9000 Series Switches Denial of Service Vulnerability	CVE-2025-20311	High	7.4
Cisco IOS XE Software Secure Boot Bypass Vulnerabilities	CVE-2025-20313 CVE-2025-20314	High	6.7
Cisco IOS and IOS XE Software CLI Denial of Service Vulnerability	CVE-2025-20149	Medium	6.5
Cisco IOS XE Software Web UI Reflected Cross-Site Scripting Vulnerability	CVE-2025-20240	Medium	6.1
Cisco IOS XE Software CLI Argument Injection Vulnerability	CVE-2025-20338	Medium	6
Cisco IOS XE Software for Catalyst 9800 Series Wireless Controller for Cloud Unauthenticated Access to Certificate Enrollment Service Vulnerability	CVE-2025-20293	Medium	5.3
Cisco IOS XE Software on Cisco Catalyst 9500X and 9600X Series Switches Virtual Interface Access Control List Bypass Vulnerability	CVE-2025-20316	Medium	5.3

RECOMMENDATIONS:

- Upgrade Cisco IOS to fixed version, where patching cannot be done immediately, administrators should limit SNMP access, exclude vulnerable OIDs, reset credentials, and closely monitor network devices for suspicious SNMP activity.
- For full technical details and patch guidance, refer to Cisco's official advisory.

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.

REFERNCES:

- https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75296