CERT-EU

Security Advisory 2025-035

High Vulnerability in Cisco IOS and IOS XE Software

2025-09-26 — v1.0

TLP:CLEAR

History:

- *26/09/2025 — v1.0 – Initial publication*

Summary

On September 24, 2025, Cisco released a security advisory regarding a high severity vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software. The vulnerability **is being exploited in the wild** [1].

It is recommended updating as soon as possible and conduct a compromise assessment on devices that are exposing SNMP on the Internet. It is also recommended not allowing access to SNMP over untrusted network (i.e. on the Internet).

Technical Details

The vulnerability **CVE-2025-20352**, with a CVSS score of 7.7, lies in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software and is due to a stack overflow condition in the SNMP subsystem. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks [1].

Exploitation of the vulnerability could allow the following:

- An authenticated, remote attacker with low privileges could cause a denial of service (DoS) condition on an affected device that is running Cisco IOS Software or Cisco IOS XE Software. To cause the DoS, the attacker must have the SNMPv2c or earlier read-only community string or valid SNMPv3 user credentials.
- An authenticated, remote attacker with high privileges could execute code as the root user on an affected device that is running Cisco IOS XE Software. To execute code as the root user, the attacker must have the SNMPv1 or v2c read-only community string or valid SNMPv3 user credentials and administrative or privilege 15 credentials on the affected device.

An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks.

Affected Products

This vulnerability affects Cisco devices if they are running a vulnerable release of Cisco IOS Software or Cisco IOS XE Software. Customers should use the Cisco Software Checker to determine the appropriate patched release for their specific software train [1].

Meraki MS390 and Cisco Catalyst 9300 Series Switches that are running Meraki CS 17 and earlier are also affected. This is fixed in Cisco IOS XE Software Release 17.15.4a [1].

Recommendations

It is recommended updating as soon as possible and conduct a compromise assessment on devices that are exposing SNMP on the Internet. It is also recommended not allowing access to SNMP over untrusted network (i.e. on the Internet) [1].

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte#fs