Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Cisco SNMP Flaw Exploited: Root Access at Risk

Date of Publication	Admiralty Code	TA Number
September 25, 2025	A1	TA2025296

Summary

Discovered On: 24 September 2025
Affected Products: Cisco IOS Software, Cisco IOS XE Software
Impact: A zero-day vulnerability in Cisco's IOS and IOS XE SNMP subsystem (CVE-2025-20352) is being actively exploited, allowing attackers to crash devices or gain root-level access. The flaw puts networks at serious risk, especially if SNMP is exposed to untrusted users. Cisco has released fixed software, making immediate upgrades essential, while temporary measures like restricting SNMP access, monitoring activity, and disabling vulnerable OIDs can help reduce risk until the patch is applied.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-20352	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability	Cisco IOS Software, Cisco IOS XE Software	✓	✗	✓

Vulnerability Details

#1 A high-severity zero-day vulnerability, tracked as CVE-2025-20352, has been discovered in Cisco's widely used IOS and IOS XE software. The flaw is a stack-based buffer overflow residing in the Simple Network Management Protocol (SNMP) subsystem and is confirmed to be actively exploited in the wild. This vulnerability allows attackers to manipulate the SNMP subsystem, posing severe risks to affected devices.

#2 The vulnerability can be triggered by a remote attacker. A low-privileged attacker with SNMPv2c or earlier read-only community strings or valid SNMPv3 credentials can exploit the flaw to cause a denial-of-service (DoS) condition, forcing the device to reload. More concerningly, a high-privileged attacker can exploit a stack overflow in the SNMP subsystem to execute arbitrary code with root-level privileges on Cisco IOS XE, leading to a complete system compromise. To achieve this, the attacker must have a combination of SNMP credentials and administrative or privilege 15 credentials on the affected device.

#3 Attackers are actively exploiting this SNMP flaw by first compromising local administrator credentials and then leveraging the stack overflow in the SNMP subsystem to crash devices or achieve root-level code execution. Cisco has issued fixed software releases that fully remediate the issue, and applying those updates is the only reliable fix. While there are no complete workarounds, temporary mitigations can reduce exposure: restrict SNMP access to trusted users, monitor SNMP, and disable affected OIDs; however, these steps may disrupt management features such as discovery and hardware inventory. Treat any mitigation as a stopgap and upgrade to Cisco's patched software without delay.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-20352	Cisco IOS & IOS XE Software, Meraki MS390 Switches - Meraki CS 17 and earlier, Cisco Catalyst 9300 Series Switches - Meraki CS 17 and earlier	cpe:2.3:o:cisco:ios:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*	CWE-121

Recommendations

Temporary Safeguards: Until devices are upgraded to Cisco's fixed software, administrators can apply temporary measures to reduce risk. Limit SNMP access to trusted users only and monitor activity with the show snmp host command. You can also disable affected OIDs using the snmp-server view command, though this may impact functions like device discovery and hardware inventory.

Update Cisco IOS and IOS XE immediately: If your devices run affected SNMP versions, upgrade to the fixed software release from Cisco. This is the only reliable way to fully protect your network from root-level exploits.

Limit SNMP access: Restrict SNMP to trusted users only and monitor the activities. This can help reduce risk until the update is applied.

Assume potential compromise: If attackers have exploited this vulnerability, they may have gained privileged access. Review administrative accounts, rotate passwords, and audit access to critical network systems.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
TA0040 Impact	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1078** Valid Accounts
T1059 Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation	**T1499** Endpoint Denial of Service	

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

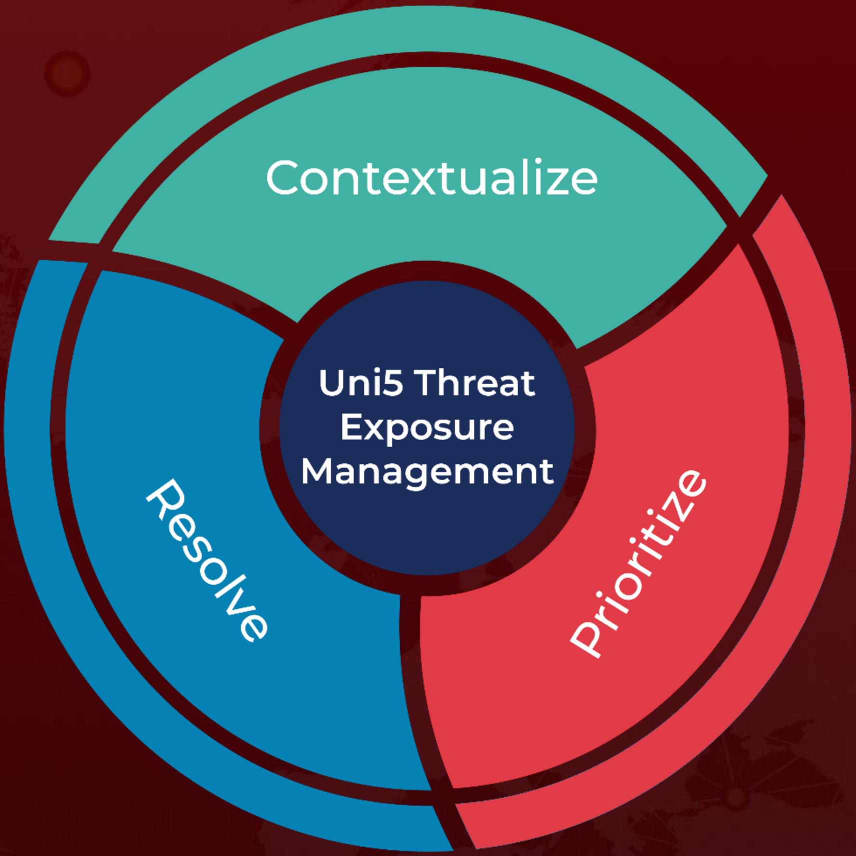
References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 25, 2025 • 9:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com