Cisco warns of IOS zero-day vulnerability exploited in attacks - Against Inv

Data: 2025-09-24 17:49:36

Autor: Inteligência Against Invaders

Cisco has released security updates to address a high-severity zero-day vulnerability in Cisco IOS

and IOS XE Software that is currently being exploited in attacks.

Tracked as CVE-2025-20352, the flaw is due to a stack-based buffer overflow weakness found in the Simple Network Management Protocol (SNMP) subsystem of vulnerable IOS and IOS XE software, impacting all devices with SNMP enabled.

Authenticated, remote attackers with low privileges can exploit this vulnerability to trigger denial-of-service (DoS) conditions on unpatched devices. High-privileged attackers, on the other hand, can gain complete control of systems running vulnerable Cisco IOS XE software by executing code as the root user.

“An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks,” Cisco said in a Wednesday advisory.

“The Cisco Product Security Incident Response Team (PSIRT) became aware of successful exploitation of this vulnerability in the wild after local Administrator credentials were compromised. Cisco strongly recommends that customers upgrade to a fixed software release to remediate this vulnerability.”

While there are no workarounds to address this vulnerability besides applying the patches released today, Cisco said that administrators who can’t immediately upgrade the vulnerable software can temporarily mitigate the issue by limiting SNMP access on an affected system to trusted users.

“To fully remediate this vulnerability and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory,” the company warned.

Today, Cisco patched 13 other security vulnerabilities, including two for which proof-of-concept exploit code is available.

The first one, a Cisco IOS XE reflected cross-site scripting (XSS) flaw tracked as CVE-2025-20240, can be used by an unauthenticated, remote attacker to steal cookies from vulnerable devices.

The second, tracked as CVE-2025-20149, is a denial-of-service vulnerability that allows authenticated, local attackers to force affected devices to reload.

In May, the company also fixed a maximum severity IOS XE flaw impacting Wireless LAN Controllers, which enabled unauthenticated attackers to remotely take over devices using a hard-

coded JSON Web Token (JWT).

[IMAGEM REMOVIDA]