From user to root in a second! CISA warns: millions of operating systems

Data: 2025-09-30 11:41:06

Autor: Inteligência Against Invaders

Redazione RHC:**30 September 2025 13:40**

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a critical vulnerability in the popular Sudo utility, used on Linux and Unix-like systems, to its catalog of currently exploitable vulnerabilities (KEVs).

The bug is filed as CVE-2025-32463 and has **a CVSS score of 9.3** . It affects Sudo versions prior to 1.9.17p1 and allows a local user, via the -R (–chroot) option, to execute arbitrary commands as root, even if their execution is not specified in the sudoers configuration. The issue was first reported by Stratascale researcher Rich Mirch in late June 2025.

While the exact exploitation of the vulnerability and the identity of the attackers remain unclear, CISA has documented instances of exploitation in the wild. Therefore, the agency has directed federal civilian agencies to address the threat by October 20, 2025, to reduce the risk of network compromise.

In addition to the Sudo bug, four other vulnerabilities have been added to the KEV list. The first is CVE-2021-21311 in the Adminer tool, which relates to server-side SSRF.

It allows remote attackers to obtain sensitive data and was previously exploited by the UNC2903 group against AWS infrastructure, as reported by Google Mandiant in 2022.

The second is CVE-2025-20352 in Cisco IOS and IOS XE. This vulnerability in the SNMP subsystem can lead to both denial of service and arbitrary code execution; Cisco confirmed its exploitation last week.

The third vulnerability is CVE-2025-10035 in Fortra GoAnywhere MFT. It causes insecure deserialization and could allow object substitution and subsequent command injection if an attacker uses a forged license response.

This activity was discovered by watchTowr Labs. The latest vulnerability is CVE-2025-59689 in Libraesva Email Security Gateway. This flaw allows command injection via compressed email attachments; exploitation has been confirmed by the vendor.

CISA emphasizes that *the presence of such entries in KEV indicates a high likelihood of attacks against organizations that have not installed the updates* . Vendors and administrators are advised to immediately fix these vulnerabilities, as they already pose a significant threat.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli