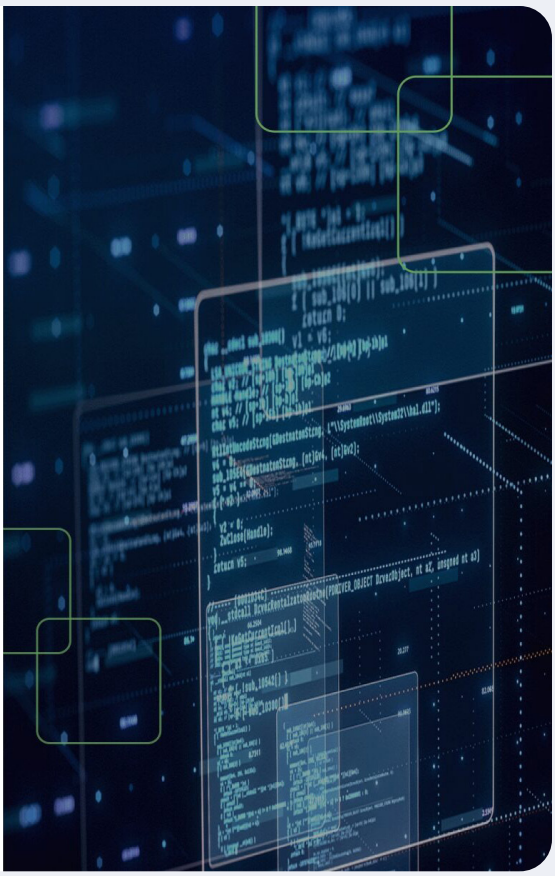
Dataminr | NEWCOM Authorized Partner

CVE-2025-9491: Exploitable Vulnerability in Sudo

On September 29, 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-32463 to its Known Exploited Vulnerabilities (KEV) catalog.



Overview of the Vulnerability

On September 29, 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-32463 to its Known Exploited Vulnerabilities (KEV) catalog. This is a critical local privilege escalation vulnerability affecting the Sudo binary, which is fundamental to Linux system administration.

The vulnerability enables local users with low-level privileges to escalate their access to root level, effectively compromising the entire system and allowing lateral movement across the network. This type of privilege escalation attack poses significant risks to organizations running vulnerable versions of Sudo across their Linux infrastructure.

The vulnerability, with a CVSS score of 9.3, affects Sudo versions 1.9.14 through 1.9.17 and has existed since June 2023, when version 1.9.14 was released. Popular affected Linux distros include Alpine Linux, Amazon Linux, Debian, Gentoo, Red Hat, SUSE, and Ubuntu. Organizations running these specific versions face immediate risk from potential attackers who could leverage this flaw to gain unauthorized root access.

Author
Jeanette Miller-Osborn, Field Cyber Intelligence Officer

OCTOBER 28, 2025

Key Takeaways

- CVE-2025-32463 is a critical local privilege escalation vulnerability affecting the Sudo binary that enables local users with low-level privileges to escalate their access to root level.
- Threat actors have actively exploited the vulnerability since at least July 2025.
- On July 4, 2025, Dataminr's AI platform detected numerous instances of this vulnerability in more than 20 languages.

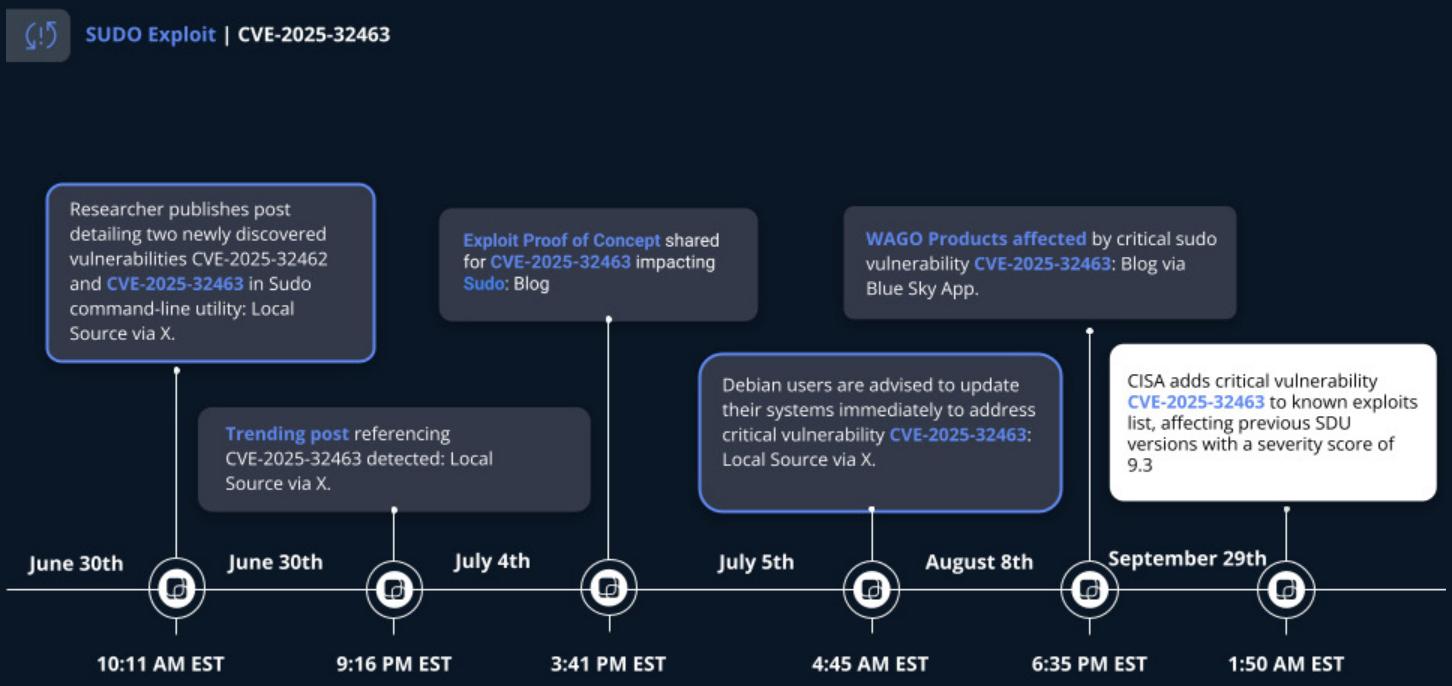
To learn more, contact **NEWCOM**
781.826.7989 | sales@newcomglobal.com
NEWCOMGlobal.com

NEWCOM

Dataminr's Detection

The vulnerability was first disclosed by Stratascale researcher Rich Mirch on June 30, 2025 with a subsequent Proof of Concept (PoC) published 4 July 2025. Threat actors have actively exploited the vulnerability since at least July 2025 with additional PoCs published publicly.

Dataminr's AI platform detected numerous instances of this vulnerability in more than 20 languages beginning the day it was disclosed. The news quickly spread amongst the cybersecurity community within the US, EMEA, and APAC with a spike in traffic in early July. However, it largely disappeared from online discussion and was not featured in mainstream media until CISA added it to the KEV catalog in late September.



Timeline of notification and alerting from the day of original disclosure.

Dataminr's Recommendations

To protect their infrastructure from exploitation, security teams can take the following steps:

- Immediately patch and check system logs for CHROOT= for potential malicious activity.
- Follow CISA's guidance to federal agencies, even if in the private sector, to apply official mitigations by installing Sudo 1.9.17p1 or later, or discontinue Sudo's use by October 20, 2025.

ReGenAI

Intel Agents

Cyber context

- **Background and Exploit Status:** A critical vulnerability, CVE-2025-32463 (CVSS: 9.3), affects the Sudo command-line utility, impacting Linux distributions with versions prior to 1.9.17p1. A proof-of-concept exploit is available, and the vulnerability is being actively exploited.
- **Impact:** This vulnerability is locally exploitable, requiring access to a user-controlled directory, and can lead to root access and potential data breaches.
- **Recommendations and Response:** CISA recommends an update to Sudo version 1.9.17p1, particularly for Linux-based systems in the IT sector, as it has been added to the Known Exploited Vulnerabilities catalog.

Discovered entities (1) *CVE-2025-32463*

Understand how Dataminr's real-time event, threat & risk intelligence empowers your organization to preemptively defend against cyber threats.

@ 2025 Dataminr. All rights reserved