THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Surge in Privilege Escalation Vulnerabilities Targeting Linux Systems

[CVE-2025-32463 | CVE-2025-32462]

CATEGORY

Vulnerability

SEVERITY

Critical

Platforms

Linux

IMPACT

- Operational Impact
- Privilege Escalation
- Exploitation Impact
- MITRE ATT&CK-Based Impact

Description

Surge in Privilege Escalation Vulnerabilities Targeting Linux Systems

A new wave of local privilege escalation (LPE) vulnerabilities has been discovered targeting the Sudo utility on widely used Linux distributions. Tracked as CVE-2025-32462 and CVE-2025-32463, these flaws can be exploited to gain unauthorized root access, potentially leading to full system compromise.

These vulnerabilities follow the recent disclosure of CVE-2025-6018 and CVE-2025-6019, and are part of a broader trend in 2025 a 34% rise in exploitation-based intrusions, with over 24,500 vulnerabilities disclosed year-to-date. These developments signal an increased risk for Linux systems and demand immediate attention from defenders.

Technical Summary:

CVE-2025-32463 (Critical)

- **Component:** --chroot (-R) option in Sudo
- **Impact:** Allows execution of commands in a controlled root path
- **Exploit Mechanism:**
  - Attackers can place a malicious /etc/nsswitch.conf in the chroot path.
  - If supported, this forces Sudo to load malicious shared libraries, escalating privileges to root.
- **Affected Versions:** 1.9.14 to 1.9.17
- **Not Affected:** Versions prior to 1.9.14

CVE-2025-32462 (Medium)

- **Component:** --host (-h) flag misuse
- **Impact:** Allows command execution across unauthorized host rules
- **Exploit Mechanism:**
  - Improper enforcement allows attackers to bypass hostname-based sudoers restrictions, resulting in root access under specific sudo rules.
- **Affected Versions:**
  - Stable: 1.9.0 to 1.9.17
  - Legacy: 1.8.8 to 1.8.32

Recommended Immediate Actions

Update Immediately

- Upgrade to Sudo version 1.9.17p1, which addresses both vulnerabilities.
- Major Linux vendors (Ubuntu, Debian, Fedora, SUSE) have already released patches.

❌ **No Workarounds Exist**

- Patching is the only effective mitigation method.

🔒 **Hardening Measures**

- Regularly audit sudoers files for misuse of --host or --chroot permissions.
- Avoid assigning elevated privileges without strict hostname/path constraints.

🧠 **Proactive Detection & Threat Hunting**

- Monitor for abuse of the sudo binary, especially use of -R and -h flags.
- Deploy updated Sigma rules from trusted platforms like SOC Prime to detect exploit attempts.

ThreatCure

Cyber Threat Advisory

Secure your byte world

Surge in Privilege Escalation Vulnerabilities Targeting Linux Systems

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net