INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-04 06:07 UTC

Rocky Linux RLSA-2026-12345: Critical sudo Privilege Escalation Vulnerability (CVE-2026-35535)

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0117
Type	CVE Vulnerability
CVE ID	CVE-2026-35535
Severity	CRITICAL
EPSS Score	0.0001 (0th percentile)
Affected Products	Rocky Linux 9 (sudo package); likely affects Red Hat Enterprise Linux 9 and downstream distributions including Oracle Linux, Ubuntu (scope unconfirmed pending authoritative source verification)
Published	2026-05-03
Discovery Source	Gemini

Executive Summary

A critical privilege escalation vulnerability has been identified in the sudo package on Rocky Linux 9, tracked as CVE-2026-35535 and addressed by Rocky Linux Security Advisory RLSA-2026-12345. An attacker with local access to an affected system could escalate to root-level privileges, potentially compromising the entire host. Note: Full technical specifics including CVSS score and confirmed attack vector have not yet been verified from authoritative NVD or vendor records; this advisory is based on Rocky Linux Security Advisory RLSA-2026-12345 and distribution-level corroboration only.

Technical Analysis

CVE-2026-35535 is a reported critical privilege escalation vulnerability in the sudo package affecting Rocky Linux 9, addressed via RLSA-2026-12345. The vulnerability class maps to CWE-269 (Improper Privilege Management) and aligns with MITRE ATT&CK technique T1548.003 (Sudo and Sudo Caching). Historical sudo privilege escalation flaws (e.g., CVE-2021-3156 'Baron Samedit') have involved argument parsing or heap overflow conditions allowing local users to gain root without valid credentials. CAUTION: Technical specifics for this CVE are unconfirmed. CVSS base score, CVSS vector, CWE confirmation, and exact attack vector were not retrievable from NVD at analysis time (CVE-2026-35535 may be newly reserved or not yet fully populated). Confirmed affected scope: Rocky Linux 9 sudo package (per RLSA-2026-12345). Suspected but unconfirmed

scope: Red Hat Enterprise Linux 9 and downstream distributions including Oracle Linux and Ubuntu. Patch: Apply the update delivered via RLSA-2026-12345 through standard Rocky Linux package management. Monitor NVD entry https://nvd.nist.gov/vuln/detail/CVE-2026-35535 (currently incomplete) and the Red Hat Customer Portal https://access.redhat.com/security/cve/cve-2026-35535 for authoritative technical detail as records populate. All severity characterizations here are inferred from vulnerability class and historical precedent, not sourced from confirmed vendor CVSS data. Confidence: LOW for all technical specifics. CWE-269 is assigned based on vulnerability class; once NVD publishes full technical details, verify whether more specific CWEs (e.g., CWE-78, CWE-94) apply based on the actual attack mechanism.

Action Checklist

1. Step 1: Containment, Identify all Rocky Linux 9 systems in your environment running the sudo package. Prioritize internet-facing systems, jump hosts, and systems with broad user access. Where operationally feasible, restrict local login access to sudo-enabled accounts until patching is confirmed; consider alternative controls such as MFA or session logging if full restriction is not possible.
2. Step 2: Detection, Query your asset inventory for Rocky Linux 9 hosts. Run 'rpm -q sudo' on candidate systems to confirm package version. Review /var/log/secure (or journalctl -u sudo) for unexpected sudo invocations, particularly from non-administrative accounts or at unusual hours. No confirmed IOC patterns are available for this CVE at this time.
3. Step 3: Eradication, Apply the patched sudo package delivered via RLSA-2026-12345 using 'dnf update sudo' on all affected Rocky Linux 9 systems. Verify the installed version resolves the advisory.
4. Step 4: Recovery, After patching, confirm the updated sudo version is installed ('rpm -q sudo'). Review sudoers configuration for unnecessary privilege grants. Monitor /var/log/secure for continued anomalous sudo activity for at least 72 hours post-patch.
5. Step 5: Post-Incident, Assess whether privileged access management (PAM) controls, least-privilege sudoers configurations, and patch cadence SLAs are sufficient. This vulnerability class (local privilege escalation via sudo) indicates a control gap if standard users have broad sudo access. Review sudo rules and consider just-in-time privilege tools as a compensating control.
6. Multi-Distribution Considerations: For RHEL 9 and downstream distributions (Oracle Linux, Ubuntu), monitor respective vendor advisories for CVE-2026-35535 remediation guidance before applying cross-distribution updates.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to immediate if forensic review of `/var/log/secure` or `audit.log` reveals a non-administrative account successfully invoked sudo and obtained a root shell (indicated by `COMMAND=/bin/bash`, `COMMAND=/bin/sh`, or `euid=0` process spawned from a non-root UID) on any internet-facing system, jump host, or system processing PII/PHI, as this constitutes confirmed privilege escalation and potential unauthorized access requiring breach notification assessment.

Recovery Notes	After applying the RLSA-2026-12345 sudo patch, verify the fixed version is installed on every Rocky Linux 9 host using `rpm -q sudo` and cross-reference against the specific fixed package version listed in the Rocky Linux errata before declaring systems clean. Monitor `/var/log/secure` for sudo COMMAND entries from non-administrative UIDs for a minimum of 72 hours post-patch, as a threat actor who escalated prior to patching may have implanted persistence (e.g., a root-owned cron job, modified `/etc/passwd`, or a setuid shell at an unexpected path) that will survive the sudo fix. Run `find / -perm -4000 -user root -type f 2>/dev/null` post-patch to enumerate setuid binaries and compare against a known-good baseline to detect any attacker-installed setuid backdoors.
Forensic Artifacts	/var/log/secure and /var/log/secure-* (rotated): Contains all sudo invocation records including USER, COMMAND, PWD, and authentication failure events — primary source for detecting exploitation of CVE-2026-35535 via unexpected privilege escalation by non-admin UIDs | /var/log/audit/audit.log filtered for type=SYSCALL with uid!=0 and euid=0: Captures the kernel-level privilege transition that a successful sudo privilege escalation exploit would produce, providing evidence of the exact UID that gained root | Output of 'rpm -V sudo' on affected systems: Detects any in-place modification of the sudo binary (hash mismatch flagged as '..5.....') that could indicate an attacker replaced or patched the binary after exploiting CVE-2026-35535 to maintain persistence | /etc/sudoers and /etc/sudoers.d/* snapshot at time of discovery: Preserves the exact privilege grant configuration that was in effect during the vulnerability window, establishing whether broad NOPASSWD or ALL=(ALL) ALL rules existed that amplified the exploitability of CVE-2026-35535 | Output of 'find / -perm -4000 -user root -type f 2>/dev/null' compared against a pre-incident baseline: Identifies attacker-planted setuid binaries (e.g., a setuid copy of /bin/bash at /tmp/.x or /usr/local/bin/) that a threat actor may have dropped after escalating to root via the vulnerable sudo package

Per-Action IR Details

Step 1: Containment — Identify all Rocky Linux 9 systems in your environment running the sudo package. Prioritize internet-facing systems, jump hosts, and systems with broad user access. Restrict local login access to sudo-enabled accounts where operationally feasible until patching is confirmed.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-6 (Least Privilege), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Run the following one-liner across all reachable Rocky Linux 9 hosts via SSH to enumerate affected systems: `for host in $(cat hosts.txt); do ssh $host 'hostname && rpm -q sudo'; done`. Pipe output to a file and filter for versions preceding the RLSA-2026-12345 fixed build. To restrict sudo access without full lockout, comment out broad sudoers rules temporarily using `visudo` and replace with explicit per-command allowances: `%wheel ALL=(ALL) /usr/bin/specific_command_only`. Use `pam_access` in `/etc/security/access.conf` to restrict interactive logins to named admin accounts on jump hosts.

Evidence: Before restricting access, capture the current sudoers configuration (`visudo -c && cat /etc/sudoers && ls -la /etc/sudoers.d/`) and a snapshot of all accounts with sudo rights (`getent group wheel sudo`). Capture `/var/log/secure` and `/var/log/auth.log` (if present) covering the 30 days prior to advisory publication. Record currently logged-in sessions (`who -a`, `last`, `w`) and active processes running as root (`ps -ef | grep -v grep | awk '$1=="root"'`) to establish a pre-containment baseline for later comparison.

Step 2: Detection — Query your asset inventory for Rocky Linux 9 hosts. Run 'rpm -q sudo' on candidate systems to confirm package version. Review /var/log/secure (or journalctl -u sudo) for unexpected sudo invocations, particularly from non-administrative accounts or at unusual hours. No confirmed IOC patterns are available for this CVE at this time.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Query `/var/log/secure` for sudo activity with: `grep -E 'sudo.*COMMAND|sudo.*authentication failure|sudo.*NOT in sudoers' /var/log/secure | awk '{print $1,$2,$3,$5,$14}' | sort`. Identify non-admin accounts invoking sudo: `grep 'sudo' /var/log/secure | grep -v 'root\|admin\|sysadmin' | grep COMMAND`. For auditd-enabled systems, query the audit log for setuid/setgid execution: `ausearch -m EXECVE,SYSCALL -c sudo --start recent`. Install and configure auditd rules to capture privilege escalation attempts if not already present: `auditctl -a always,exit -F arch=b64 -S execve -F uid!=0 -F euid=0 -k priv_esc_cve_2026_35535`. Because no confirmed IOC signatures exist for this CVE at time of advisory, treat any non-admin sudo COMMAND entries in `/var/log/secure` post-dating the advisory's affected version installation as a high-suspicion indicator requiring manual triage.

Evidence: Collect `/var/log/secure` and `/var/log/secure-*` (rotated logs) covering the period from initial sudo package installation to present, parsed for `sudo` entries. Run `journalctl -u sudo --since '30 days ago' --no-pager > sudo_journal_export.txt`. Capture `rpm -q --queryformat '%{INSTALLTIME:date}\n' sudo` to confirm when the vulnerable version was installed. Extract `/var/log/audit/audit.log` entries for `type=EXECVE` where `uid!=0` and `euid=0`, which would indicate a successful privilege escalation if this vulnerability involves a setuid mechanism. Preserve `/proc//status` for any suspicious root-owned processes not present in the pre-containment baseline.

Step 3: Eradication — Apply the patched sudo package delivered via RLSA-2026-12345 using 'dnf update sudo' on all affected Rocky Linux 9 systems. Verify the installed version resolves the advisory. For RHEL 9 and downstream distributions, monitor respective vendor advisories before applying cross-distribution updates.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For systems without automated patch management, apply the fix manually: `dnf clean all && dnf update sudo -y && rpm -q sudo --queryformat '%{NAME}-%{VERSION}-%{RELEASE}.%{ARCH}\n'`. Verify the installed version matches the fixed build specified in RLSA-2026-12345 by comparing against the Rocky Linux Errata page at https://errata.rockylinux.org (human-validated URL recommended). For air-gapped systems, download the RPM from the Rocky Linux mirrors and verify the package signature before installing: `rpm --checksig sudo-.rpm`. Do NOT apply Rocky Linux RPMs to RHEL 9 or Oracle Linux 9 — wait for Red Hat RHSA and Oracle ELSA advisories respectively, as package builds differ despite upstream compatibility.

Evidence: Before running `dnf update sudo`, capture the pre-patch package state: `rpm -qi sudo > sudo_pre_patch_state.txt`. After patching, capture `rpm -qi sudo > sudo_post_patch_state.txt` and diff both files to confirm version change. Preserve `dnf history info ` output documenting the patch transaction with timestamp. If a suspected exploitation occurred prior to patching, preserve a memory image of the running system using `avml` or `LiME` before rebooting, as a successful local privilege escalation via sudo may have left a root-owned process or modified setuid binary that will not survive a service restart.

Step 4: Recovery — After patching, confirm the updated sudo version is installed ('rpm -q sudo'). Review sudoers configuration for unnecessary privilege grants. Monitor /var/log/secure for continued anomalous sudo activity for at least 72 hours post-patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Validate sudoers hygiene by running `visudo -c` to confirm syntax integrity, then audit for overbroad rules: `grep -E 'ALL.*ALL.*ALL|NOPASSWD' /etc/sudoers /etc/sudoers.d/*`. Flag any `NOPASSWD` entries for non-service accounts for immediate remediation, as these would have lowered the bar for exploiting CVE-2026-35535 by removing the password prompt barrier. Set up a 72-hour continuous monitoring cron job: `*/15 * * * * grep 'sudo.*COMMAND' /var/log/secure | grep -v root > /tmp/sudo_monitor_$(date +\%Y\%m\%d\%H\%M).log` and review aggregated output daily. Use `rpm -V sudo` to verify the installed sudo binary matches the expected RPM manifest (file size, hash, permissions) and detect any in-place binary tampering that may have occurred before patching.

Evidence: Capture `/etc/sudoers` and all files under `/etc/sudoers.d/` immediately after patching and store as a configuration baseline. Run `rpm -V sudo` and preserve output — any deviation (e.g., `..5.....` indicating an MD5 mismatch on the sudo binary) is evidence of potential pre-patch tampering. Collect 72 hours of post-patch `/var/log/secure` entries filtered for sudo, preserving both COMMAND (successful) and authentication failure (failed) lines, to confirm no continued exploitation attempts against the now-patched binary.

Step 5: Post-Incident — Assess whether privileged access management (PAM) controls, least-privilege sudoers configurations, and patch cadence SLAs are sufficient. This vulnerability class (local privilege escalation via sudo) indicates a control gap if standard users have broad sudo access. Review sudo rules and consider just-in-time privilege tools as a compensating control.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For just-in-time (JIT) privilege without commercial PAM tooling, implement `sudo` with tightly scoped `Cmnd_Alias` blocks per role and enable `sudo` logging to a remote syslog target so local root cannot tamper with evidence. Evaluate open-source tools: `tlog` (session recording for privileged access, available in RHEL/Rocky repos) and `sudoreplay` (built into sudo) for privileged session audit trails. Establish a patch SLA policy requiring Critical-severity sudo/kernel privilege escalation CVEs be remediated within 72 hours of advisory publication on all internet-facing and jump host systems, documented in the IR plan per NIST IR-8 (Incident Response Plan).

Evidence: Produce a post-incident lessons-learned record documenting: (1) the time delta between RLSA-2026-12345 publication and full patch deployment across the Rocky Linux 9 estate, (2) the count of systems found with `NOPASSWD` or `ALL=(ALL) ALL` sudoers rules at time of discovery, and (3) whether any `/var/log/secure` entries indicated exploitation activity during the exposure window. This record feeds directly into patch cadence SLA review and supports NIST AU-11 (Audit Record Retention) requirements for incident documentation.

Detection Guidance

Note: These detection methods assume Linux audit logging (auditd) and SELinux/AppArmor are enabled and properly configured. Organizations without these controls should prioritize patching and access restriction. No confirmed IOCs or exploit-specific behavioral signatures are available for CVE-2026-35535 at this time; NVD and vendor records were not fully populated at analysis. General detection guidance for sudo privilege escalation: (1) Monitor /var/log/secure or journalctl output for sudo invocations by non-administrative accounts, repeated authentication failures, or sudo usage outside business hours. (2) Alert on Linux audit log event type SYSCALL where comm='sudo' combined with unexpected UID changes (auid != 0 escalating to uid=0). (3) Use auditd rules targeting execve calls involving sudo binary (/usr/bin/sudo) with unusual argument patterns. (4) EDR/SIEM: Correlate process creation events where parent process is sudo and child process is a shell (bash, sh, zsh) launched as root from a non-root initiating user. Revisit detection specifics once NVD and vendor advisories publish confirmed attack vector and exploit details.

Framework Mappings

MITRE-ATTACK

- **T1548.003** — Sudo and Sudo Caching

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

NIST-800-53R5

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548.003	Sudo and Sudo Caching	Privilege-Escalation

Sources

Source	URL	Tier
CVE-2026-35535 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-35535	T1
Vulnerability Details : CVE-2026-35535	https://www.cvedetails.com/cve/CVE-2026-35535/	T3

Source	URL	Tier
CVE-2026-35535 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-35535	**T3**
CVE-2026-35535 - Ubuntu	https://ubuntu.com/security/CVE-2026-35535	**T3**
Oracle Linux: CVE-2026-35535 - Rapid7 Vulnerability Database	https://www.rapid7.com/db/vulnerabilities/oracle_linux-cve-2026-35535/	**T3**

Generated 2026-05-04 06:07 UTC by TJS Security Command Center