INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 06:59 UTC

CVE-2026-46333: Nine-Year Linux Kernel Flaw Delivers Reliable Root Access Across Major Distributions

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0206
Type	CVE Vulnerability
CVE ID	CVE-2026-46333
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0001 (0th percentile)
Affected Products	Linux kernel versions from November 2016 onward; Debian, Fedora, and Ubuntu default installations; affected SUID binaries: chage, ssh-keysign, pkexec, accounts-daemon
Published	2026-05-21T03:35:53
Discovery Source	Rss

Executive Summary

A nine-year-old privilege escalation flaw in the Linux kernel (CVE-2026-46333) allows any local user to gain full root access on default installations of Debian, Fedora, and Ubuntu. A public proof-of-concept is available with four confirmed exploit chains, and successful exploitation also exposes password hashes and SSH host private keys. Organizations running unpatched Linux systems face risk of complete host compromise, credential theft, and lateral movement across their environment.

Technical Analysis

CVE-2026-46333 is a privilege escalation vulnerability in the Linux kernel's __ptrace_may_access() function, introduced approximately November 2016 and present across roughly nine years of kernel releases. The flaw is exploitable locally by an unprivileged user against default installations of Debian, Fedora, and Ubuntu. Four confirmed exploit chains have been identified targeting SUID binaries: chage, ssh-keysign, pkexec, and accounts-daemon. A public proof-of-concept is available. Successful exploitation yields arbitrary command execution as root (T1068, T1548.001), access to /etc/shadow exposing password hashes (T1003.008, T1552.001), and SSH host private key exposure (T1552.004). Associated CWEs: CWE-269 (Improper Privilege Management), CWE-416 (Use After Free), CWE-284 (Improper Access Control). CVSS base score is 7.5. EPSS score is 7e-05 (0.00439th percentile) as of data capture, but EPSS is a lagging indicator and does not yet

reflect PoC publication. Not currently listed in CISA KEV. Patch status: apply vendor-specific kernel updates from Debian, Fedora, Red Hat, and Ubuntu security channels. Reference: NVD entry at https://nvd.nist.gov/vuln/detail/CVE-2026-46333 (authoritative source, NIST NVD).

Action Checklist

1. Step 1: Containment. Audit all Linux systems running kernel versions from November 2016 onward; restrict local shell access and SSH access to only authorized accounts on affected Debian, Fedora, and Ubuntu hosts immediately. Restrict or remove SUID bits on chage, ssh-keysign, pkexec, and accounts-daemon where possible using 'chmod u-s' pending patching. Enforce least privilege per NIST AC-6 and CIS 5.4.
2. Step 2: Detection. Search for ptrace-related syscall anomalies in kernel audit logs (auditd rules targeting ptrace, execve by unexpected users, and SUID binary invocations). Query SIEM for processes spawned as UID 0 from non-root parent processes. Review /var/log/auth.log and /var/log/secure for unexpected privilege changes. Monitor for unauthorized reads of /etc/shadow and SSH key material in /etc/ssh/. Reference NIST AU-6 and AU-12; CIS 8.2.
3. Step 3: Eradication. Apply the vendor-issued kernel security update for your distribution: Ubuntu Security Notice (consult https://ubuntu.com/security/notices and search for CVE-2026-46333), Debian Security Advisory (consult https://www.debian.org/security/ for CVE-2026-46333), Fedora/Red Hat errata via https://access.redhat.com/security/cve/cve-2026-46333. Verify installed kernel version post-update. Where patching is not immediately possible, disable or restrict SUID binaries chage, ssh-keysign, pkexec, and accounts-daemon. Reference NIST SI-2; CIS 7.3.
4. Step 4: Recovery. After patching, rotate all local account passwords and SSH host keys on affected systems; /etc/shadow and SSH host private keys must be treated as compromised on any system that was accessible to unprivileged local users prior to patching. Re-issue SSH host certificates where applicable. Validate kernel version and SUID binary permissions post-change. Monitor for re-exploitation attempts per NIST IR-4 and AU-6. Apply credential rotation and credential hardening controls.
5. Step 5: Post-Incident. Review privileged access controls for all Linux hosts; enforce MFA for SSH and administrative access per CIS 6.4 and CIS 6.5. Implement automated patch management cadence for kernel updates per CIS 7.3. Assess whether auditd or equivalent kernel-level monitoring was in place and close gaps per NIST AU-2 and AU-12. Evaluate whether local account monitoring and system file analysis controls are implemented for future detection of similar local privilege escalation attempts.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if any evidence exists that /etc/shadow was read by a non-root process (indicating password hash exfiltration), SSH host keys in /etc/ssh/ were accessed by non-root users (enabling impersonation or MitM of other systems), or if affected systems handle PII, PHI, or payment card data triggering breach notification obligations under GDPR, HIPAA, or PCI-DSS; additionally escalate if the public PoC with four confirmed exploit chains is observed in logs prior to patch deployment, indicating active exploitation rather than exposure.

Recovery Notes	All Linux systems that were running a vulnerable kernel (any version from November 2016 onward, unpatched through CVE-2026-46333 remediation) and were accessible to any unprivileged local user must be treated as having had /etc/shadow and all SSH host private keys exposed — credential rotation is mandatory, not precautionary. After patching and key rotation, maintain heightened monitoring of auditd logs for ptrace and SUID binary invocations and of /var/log/auth.log for root session initiations for a minimum of 30 days, as attackers with prior access may have planted cron-based or systemd-based persistence that survives the kernel patch. Validate the integrity of /etc/crontab, /etc/cron.d/, /var/spool/cron/crontabs/, and systemd unit files in /etc/systemd/system/ and /usr/local/lib/systemd/system/ on all affected hosts, as root-level persistence implanted before the patch is not removed by the kernel update itself.
Forensic Artifacts	auditd SYSCALL records for ptrace (syscall=101 on x86_64, syscall=26 on x86) initiated by processes with auid>=1000 — the core kernel mechanism CVE-2026-46333 exploits to achieve privilege escalation from unprivileged local user to UID 0 | /var/log/auth.log or journalctl -u sshd entries showing 'session opened for user root by (uid=)' — direct evidence of successful privilege escalation to root, distinct from legitimate root logins which originate from UID 0 parent processes | auditd file-watch records for reads of /etc/shadow (password hashes) and /etc/ssh/ssh_host_*_key (SSH host private keys) by processes owned by non-root UIDs — this exploit's post-escalation impact is specifically the exposure of these two credential stores | Process ancestry records from 'ps -eo pid,ppid,euid,ruid,user,cmd' or Sysmon for Linux ProcessCreate events showing root-effective-UID processes (euid=0) spawned from one of the four confirmed SUID exploit chain binaries: chage, ssh-keysign, pkexec, or accounts-daemon, with a non-root real UID (ruid>=1000) parent | Kernel ring buffer output from 'dmesg' and /var/log/kern.log capturing any kernel NULL pointer dereference, use-after-free, or unexpected capability grants — kernel-level privilege escalation exploits frequently produce kernel warning or oops messages in the ring buffer that correlate with the exploitation timestamp

Per-Action IR Details

Step 1: Containment — Audit all Linux systems running kernel versions from November 2016 onward; restrict local shell access and SSH access to only authorized accounts on affected Debian, Fedora, and Ubuntu hosts immediately. Restrict or remove SUID bits on chage, ssh-keysign, pkexec, and accounts-daemon where operationally feasible using 'chmod u-s' pending patching. Enforce least privilege per NIST AC-6 and CIS 5.4.

NIST Phase: Containment

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'find / -perm -4000 -type f 2>/dev/null' on each affected host to enumerate all SUID binaries and confirm current state before modification. Execute 'chmod u-s /usr/bin/chage /usr/bin/ssh-keysign /usr/bin/pkexec /usr/sbin/accounts-daemon' to remove SUID bits on the four confirmed exploit-chain binaries. Restrict SSH to a jump host or named admin accounts using AllowUsers or AllowGroups in /etc/ssh/sshd_config, then 'systemctl reload sshd'. Use 'lastlog' and 'who' to identify currently active non-root sessions and terminate suspicious ones with 'pkill -KILL -u '.

Evidence: Before removing SUID bits, document the pre-change permission state with 'stat /usr/bin/chage /usr/bin/ssh-keysign /usr/bin/pkexec /usr/sbin/accounts-daemon > /tmp/suid_baseline_$(date +%F).txt'. Capture current UID-0 process list with 'ps aux | awk "$1 == \"root\""' and preserve /etc/passwd and /etc/shadow hashes (read-only copy) as they may reflect accounts created via root access gained through the exploit. Record active SSH sessions from /var/log/auth.log or journalctl targeting sshd entries in the 24-48 hours prior to containment — these may reveal the attacker's entry account used to stage local privilege escalation via pkexec or chage.

Step 2: Detection — Search for ptrace-related syscall anomalies in kernel audit logs (auditd rules targeting ptrace, execve by unexpected users, and SUID binary invocations). Query SIEM for processes spawned as UID 0 from non-root parent processes. Review /var/log/auth.log and /var/log/secure for unexpected privilege changes. Monitor for unauthorized reads of /etc/shadow and SSH key material in /etc/ssh/. Reference NIST AU-6 and AU-12; CIS 8.2.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy auditd rules immediately targeting this exploit's mechanism: 'auditctl -a always,exit -F arch=b64 -S ptrace -k cve_2026_46333_ptrace' and 'auditctl -a always,exit -F arch=b64 -S execve -F euid=0 -F auid>=1000 -k privesc_root'. Add file-access watches on /etc/shadow and /etc/ssh/ with 'auditctl -w /etc/shadow -p r -k shadow_read' and 'auditctl -w /etc/ssh/ -p r -k sshkey_read'. For SUID binary invocations without a SIEM, run: 'ausearch -k cve_2026_46333_ptrace | aureport -f -i' to parse kernel audit logs. Install Sysmon for Linux (Microsoft Sysmon for Linux on GitHub) and configure it to log ProcessCreate events where ParentUser differs from User and UID transitions to 0.

Evidence: Pull auditd logs for SYSCALL records showing ptrace (syscall=101 on x86_64) initiated by processes owned by non-root UIDs (auid>=1000) — this is the kernel-level mechanism CVE-2026-46333 exploits. Search /var/log/auth.log or 'journalctl -u sshd --since -7days' for 'session opened for user root' events preceded immediately by a non-root user's login, indicating successful UID 0 elevation. Check for unexpected reads of /etc/shadow using 'ausearch -f /etc/shadow' — legitimate shadow reads are rare outside of passwd/chage operations and a non-root process reading this file is a strong compromise indicator. Inspect process ancestry trees with 'ps -eo pid,ppid,euid,user,cmd' looking for root-owned processes with non-root parent PIDs, consistent with SUID exploit chain execution.

Step 3: Eradication — Apply the vendor-issued kernel security update for your distribution: Ubuntu Security Notice (check https://ubuntu.com/security/notices), Debian Security Advisory (check https://www.debian.org/security/), Fedora/Red Hat errata via https://access.redhat.com/security/cve/cve-2026-46333. Verify installed kernel version post-update. Where patching is not immediately possible, disable or restrict SUID binaries chage, ssh-keysign, pkexec, and accounts-daemon. Reference NIST SI-2; CIS 7.3.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For Ubuntu: 'sudo apt-get update && sudo apt-get install --only-upgrade linux-image-$(uname -r)' followed by 'uname -r' post-reboot to confirm patched kernel version. For Debian: 'sudo apt-get update && sudo apt-get upgrade linux-image-$(uname -r)'. For Fedora: 'sudo dnf update kernel' followed by reboot. Where reboot is not immediately possible, enforce temporary mitigation: 'systemctl stop accounts-daemon && systemctl disable accounts-daemon' if operationally acceptable, and verify SUID removal persists across package updates by pinning permissions in /etc/permissions.local (SUSE-style) or via an Ansible playbook or cron-enforced script: 'chmod u-s /usr/bin/pkexec /usr/bin/chage /usr/bin/ssh-keysign'. Verify no attacker-installed backdoor kernel modules with 'lsmod | grep -v $(cat /proc/modules | awk "{print $1}" | sort)' baseline comparison.

Evidence: Before patching, take a full memory image using LiME (Linux Memory Extractor) if the host is suspected to have been compromised — kernel-level exploits may leave artifacts in volatile memory that are lost after reboot. Record the pre-patch kernel version with 'uname -a > /tmp/kernel_pre_patch.txt' and catalog all installed kernel packages with 'dpkg -l | grep linux-image' (Debian/Ubuntu) or 'rpm -qa | grep kernel' (Fedora) as chain-of-custody documentation. Enumerate all currently loaded kernel modules with 'lsmod > /tmp/lsmod_pre_patch.txt' to detect any attacker-planted rootkit modules installed after exploitation. Verify file integrity of patched binaries post-update using

'debsums -c' (Debian/Ubuntu) or 'rpm -Va' (Fedora) to confirm no attacker-modified binaries remain.

Step 4: Recovery — After patching, rotate all local account passwords and SSH host keys on affected systems — /etc/shadow and SSH host private keys must be treated as compromised on any system that was accessible to unprivileged local users prior to patching. Re-issue SSH host certificates where applicable. Validate kernel version and SUID binary permissions post-change. Monitor for re-exploitation attempts per NIST IR-4 and AU-6. Apply D3-CRO (Credential Rotation) and D3-CH (Credential Hardening).

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 IA-5 (Authenticator Management), NIST AC-17 (Remote Access), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Regenerate SSH host keys with 'rm /etc/ssh/ssh_host_* && dpkg-reconfigure openssh-server' (Debian/Ubuntu) or 'ssh-keygen -A' (Fedora/generic). Force password rotation for all local accounts by setting chage expiry to immediate: 'for u in $(awk -F: "$3 >= 1000 {print $1}" /etc/passwd); do chage -d 0 $u; done'. After patching and key rotation, run 'uname -r' to confirm kernel version and 're-run find / -perm -4000 -type f 2>/dev/null' to confirm SUID permissions are correct post-update (vendor patches may restore SUID bits). Distribute updated SSH host key fingerprints to all users and update known_hosts on connecting clients to prevent TOFU (trust-on-first-use) bypass by an attacker who harvested the old host key.

Evidence: Before rotating SSH host keys, preserve the existing keys to /tmp/forensic_ssh_host_keys_$(hostname)_$(date +%F)/ as forensic evidence — the private keys in /etc/ssh/ssh_host_*_key may have been exfiltrated and are needed to understand the scope of potential impersonation attacks. Document /etc/shadow contents (hash values only, not cleartext) pre-rotation as baseline evidence that password hashes were accessible to the attacker. Capture successful and failed SSH authentications from /var/log/auth.log post-recovery for a 72-hour window to detect attacker attempts to reconnect using harvested credentials or stolen host keys. Verify /etc/passwd and /etc/sudoers have not been modified by the attacker to plant persistence: compare against known-good baselines using 'md5sum /etc/passwd /etc/sudoers /etc/sudoers.d/*'.

Step 5: Post-Incident — Review privileged access controls for all Linux hosts; enforce MFA for SSH and administrative access per CIS 6.4 and CIS 6.5. Implement automated patch management cadence for kernel updates per CIS 7.3. Assess whether auditd or equivalent kernel-level monitoring was in place and close gaps per NIST AU-2 and AU-12. Evaluate whether D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) are implemented for future detection of similar local privilege escalation attempts.

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy a permanent auditd ruleset targeting local privilege escalation indicators specific to this CVE class: ptrace syscall monitoring, SUID binary execution by non-root users, and shadow file reads — store rules in /etc/audit/rules.d/privesc.rules for persistence across reboots. Implement PAM-based MFA for SSH using libpam-google-authenticator (free, widely packaged) to require TOTP in addition to key-based auth, directly mitigating the local-user-to-root pivot that this CVE enables. Create a cron job or systemd timer to run weekly kernel version checks: 'uname -r | mail -s "Kernel Version Report $(hostname)" security@example.com'. Write a Sigma rule targeting auditd SYSCALL records for ptrace by auid>=1000 and contribute to your internal detection library for future local privesc CVE variants. Use OVAL definitions from the NVD or your distribution's security feed with OpenSCAP ('oscap oval eval --results oval_results.xml cve-oval.xml') for ongoing CVE-2026-46333 patch compliance verification.

Evidence: Compile a lessons-learned timeline documenting: (1) earliest kernel log evidence of ptrace-based exploitation attempts, (2) the window during which /etc/shadow and /etc/ssh/ host keys were accessible to unprivileged users (defined by the kernel install date of the vulnerable version versus the patch date), and (3) any lateral movement

indicators in SSH logs where the stolen host key or password hashes may have been used against other systems. Preserve all auditd logs, /var/log/auth.log archives, and the pre-patch shadow file copies in a write-once evidence store with chain-of-custody documentation per NIST 800-61r3 §4 post-incident evidence retention guidance. Assess whether any other hosts in the environment accepted SSH connections from the affected systems — stolen ssh-keysign output or host keys could enable man-in-the-middle attacks against hosts that trusted the compromised system's identity.

Detection Guidance

Primary detection surface is kernel audit logs via auditd. Recommended audit rules: monitor ptrace syscall usage by non-root users (example: 'auditctl -a always,exit -F arch=b64 -S ptrace -k ptrace_monitoring'); alert on execve calls resulting in UID/EUID 0 where the parent process UID was non-zero; monitor SUID binary invocations for chage, ssh-keysign, pkexec, and accounts-daemon, especially outside expected administrative workflows. In SIEM, query for process lineage anomalies: non-root parent spawning root-owned child processes. Flag unauthorized file reads against /etc/shadow and /etc/ssh/ssh_host_*_key. Behavioral indicators include unexpected root shell spawns, new cron jobs or authorized_keys entries added post-exploitation, and SSH host key changes not tied to a maintenance window. Reference NIST AU-6, AU-12; CIS 8.2; local account monitoring and system file analysis controls. Note: EPSS score is currently low (7e-05), but this is a lagging metric; PoC publication typically precedes EPSS adjustment by days to weeks. Do not use EPSS alone to deprioritize detection.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1548.001** — Setuid and Setgid
- **T1552.004** — Private Keys
- **T1552.001** — Credentials In Files
- **T1003.008** — /etc/passwd and /etc/shadow
- **T1057** — Process Discovery

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement
- **SI-16** — Memory Protection

OWASP-TOP10-2021

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

- **16.10** — Apply Secure Design Principles in Application Architectures
- **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

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1548.001	Setuid and Setgid	Privilege-Escalation
T1552.004	Private Keys	Credential-Access
T1552.001	Credentials In Files	Credential-Access
T1003.008	/etc/passwd and /etc/shadow	Credential-Access
T1057	Process Discovery	Discovery

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/9-year-old-linux-kernel-flaw-enab...	T3
CVE-2026-46333 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-46333	T1
CVE-2026-46333 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-46333	T3
Linux Kernel ptrace Exit-race Vulnerability / ssh-keysign-pwn (CVE ...	https://blog.cloudlinux.com/ptrace-exit-race-cve-2026-46333-mitigat...	T3

Source	URL	Tier
There is a FOURTH vulnerability this month. ...ssh-keysign-pwn (CVE ...	https://www.reddit.com/r/linux/comments/1teaer5/there_is_a_fourth_v...	T3

Generated 2026-05-21 06:59 UTC by TJS Security Command Center