INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-24 18:45 UTC

CVE-2026-41651 'Pack2TheRoot': 12-Year-Old PackageKit Flaw Enables Local Root Escalation Across Major Linux Distros

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0076
Type	CVE Vulnerability
CVE ID	CVE-2026-41651
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0003 (7th percentile)
Affected Products	PackageKit 1.0.2 through 1.3.4; Ubuntu Desktop 18.04, 24.04.4 LTS, 26.04 LTS beta; Ubuntu Server 22.04-24.04 LTS; Debian Desktop Trixie 13.4; Rocky Linux Desktop 10.1; Fedora 43 Desktop and Server; any Linux distribution shipping PackageKit enabled by default
Published	2026-04-24T13:28:46
Discovery Source	Rss

Executive Summary

A 12-year-old privilege escalation flaw in PackageKit, a package management service enabled by default across major Linux distributions including Ubuntu, Debian, Fedora, and Rocky Linux, allows any authenticated local user to gain full root access without authorization. Affected versions span PackageKit 1.0.2 through 1.3.4; a patch is available in version 1.3.5. A public proof-of-concept exploit is circulating, raising the operational risk for organizations running Linux desktops or servers where local user access is granted to contractors, employees, or shared systems.

Technical Analysis

CVE-2026-41651 (Pack2TheRoot) is a local privilege escalation (LPE) vulnerability in the PackageKit daemon (versions 1.0.2-1.3.4, introduced November 2014). The flaw stems from improper privilege management (CWE-269), missing authorization checks (CWE-862), and improper authentication handling (CWE-287). An authenticated local user can invoke PackageKit to install or remove system packages without proper authorization, achieving root-level execution. Attack vector is local; no network access is required. CVSS base score is reported as 8.8 in the vendor advisory; NVD assessment is pending. Human verification against NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-41651) is recommended before operational prioritization. EPSS

percentile of 0.07% reflects low observed exploitation activity at time of reporting. A functional PoC is publicly available at github.com/Vozec/CVE-2026-41651. Affected distributions include Ubuntu Desktop 18.04, 24.04.4 LTS, and 26.04 LTS beta; Ubuntu Server 22.04-24.04 LTS; Debian Desktop Trixie 13.4; Rocky Linux Desktop 10.1; Fedora 43 Desktop and Server; and any Linux distribution shipping PackageKit enabled by default. MITRE ATT&CK mappings: T1548 (Abuse Elevation Control Mechanism), T1548.003 (Sudo and Sudo Caching), T1068 (Exploitation for Privilege Escalation), T1543.002 (Systemd Service). Remediation: upgrade to PackageKit 1.3.5.

Action Checklist

1. Step 1: Containment, Identify all Linux systems running PackageKit 1.0.2-1.3.4 across your environment, prioritizing multi-user systems (developer workstations, shared servers, VDI environments). Where patching is not immediately possible, disable or mask the PackageKit service: 'systemctl disable --now packagekit' and 'systemctl mask packagekit'. Confirm with your distro vendor advisory (Ubuntu Security Notice, Debian DSA, Fedora FEDORA-2026-*, Rocky Linux errata) for version-specific guidance.
2. Step 2: Detection, Query package management logs for unexpected PackageKit invocations by non-root users. On systemd-based systems, check 'journalctl -u packagekit' for authorization bypass patterns. Look for polkit policy evaluations granting org.freedesktop.packagekit.* actions to unprivileged users (audit logs via auditd, event keyword 'type=AVC' or 'type=USER_AUTH'). Monitor for new SUID binaries, unexpected cron entries, or new user accounts created post-exploitation as indicators of follow-on activity consistent with T1543.002.
3. Step 3: Eradication, Upgrade PackageKit to version 1.3.5 using your distribution's package manager. For Ubuntu: 'sudo apt update && sudo apt install packagekit'. For Fedora: 'sudo dnf upgrade packagekit'. For Debian: apply the relevant DSA update via 'sudo apt update && sudo apt upgrade packagekit'. For Rocky Linux: apply available errata via 'sudo dnf update packagekit'. Confirm the installed version post-upgrade: 'pkcon --version'.
4. Step 4: Recovery, After patching, verify PackageKit version is 1.3.5 or later on all affected hosts. Re-enable the service only if required for operations. Review polkit rules (files under /etc/polkit-1/rules.d/ and /usr/share/polkit-1/rules.d/) for unauthorized modifications. Audit recently installed or removed packages on affected systems for the window between initial exposure (November 2014 for systems running unpatched versions) and patch application. Monitor PackageKit and polkit logs for 30 days post-remediation for anomalous authorization requests.
5. Step 5: Post-Incident, This vulnerability exposes a control gap in local privilege boundary enforcement on Linux systems. Review polkit authorization policies across all Linux endpoints and servers. Assess whether the principle of least privilege is enforced for package management operations (only admins should invoke PackageKit). Consider implementing host-based IDS rules to alert on unexpected SUID/SGID file creation and unauthorized polkit grants. Update your Linux hardening baseline (referencing CIS Benchmarks for Linux distributions) to include PackageKit service state as a configuration audit item.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal/compliance immediately if auditd or PackageKit journal logs confirm any non-root UID successfully invoked a privileged 'org.freedesktop.packagekit.*' polkit action, or if post-exploitation artifacts (unauthorized SUID binaries, new accounts, rogue cron entries, unauthorized packages) are discovered on systems storing PII, PHI, PCI data, or credentials — as this constitutes a confirmed privilege escalation incident triggering breach notification assessment under applicable regulations (GDPR Article 33, HIPAA §164.410, PCI DSS Req. 12.10.5).
Recovery Notes	After confirming PackageKit 1.3.5 is installed and the service is masked or verified clean on all affected hosts, re-enable the service only on systems where it is operationally required and only after validating polkit rule integrity via hash comparison against a known-good baseline. Monitor auditd logs for 'type=USER_AUTH' and 'type=AVC' events referencing 'org.freedesktop.packagekit.*' actions for a minimum of 30 days post-remediation, with particular attention to any non-root UID appearing in those records. Given the 12-year vulnerability window, systems that cannot provide clean package install audit trails back to their initial PackageKit deployment should be treated as potentially compromised and considered for full reimaging from a trusted baseline.
Forensic Artifacts	systemd journal for the packagekit unit ('journalctl -u packagekit -o json'): captures all D-Bus method calls to packagekitd including the caller UID — the CVE-2026-41651 bypass would surface here as a non-root UID (> 1000) being granted a privileged 'org.freedesktop.packagekit.*' action without a corresponding polkit interactive authentication prompt | auditd records of type USER_AUTH and AVC referencing polkit and packagekit ('ausearch -m USER_AUTH,AVC | grep -i packagekit'): these record the polkit authorization decision at the kernel audit level and would show the bypass granting an unprivileged user a PackageKit admin action that should have been denied under a correct polkit policy evaluation | SUID/SGID binary filesystem scan results ('find / -perm /6000 -newer /var/lib/packagekit -ls 2>/dev/null'): an attacker who gained root via CVE-2026-41651 would likely install a SUID root shell or modify an existing binary as a persistence mechanism; timestamping against the PackageKit install date scopes the search to the exploitation window | Package installation history logs ('/var/log/apt/history.log' on Debian/Ubuntu, '/var/log/dnf.log' on Fedora/Rocky): the PackageKit exploit allows unprivileged users to install arbitrary packages as root — any package install entry correlated with a non-root session in auth.log or the PackageKit journal during the exposure window is a high-confidence exploitation indicator | Polkit rules directory integrity hashes ('/etc/polkit-1/rules.d/' and '/usr/share/polkit-1/rules.d/'): a post-exploitation attacker with root access may have modified polkit rules to permanently grant PackageKit or other D-Bus privileges to an unprivileged account, creating a persistence channel that survives the PackageKit patch; any file modification timestamp newer than the last known-good configuration change is a critical artifact

Per-Action IR Details

Step 1: Containment — Identify all Linux systems running PackageKit 1.0.2–1.3.4 across your environment, prioritizing multi-user systems (developer workstations, shared servers, VDI environments). Where patching is not immediately possible, disable or mask the PackageKit service: 'systemctl disable --now packagekit' and 'systemctl mask packagekit'. Confirm with your distro vendor advisory (Ubuntu Security Notice, Debian DSA, Fedora FEDORA-2026-*, Rocky Linux errata) for version-specific guidance.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Run 'ssh user@host pkcon --version 2>/dev/null || dpkg -l packagekit 2>/dev/null || rpm -q packagekit 2>/dev/null' in a parallel loop across all managed hosts using a bash script over your existing SSH inventory. For asset discovery without SIEM, use osquery: 'SELECT name, version FROM deb_packages WHERE name = "packagekit";' or 'SELECT name, version FROM rpm_packages WHERE name = "packagekit";'. Immediately mask the service on all vulnerable hosts via Ansible ad-hoc: 'ansible all -m systemd -a "name=packagekit state=stopped enabled=no masked=yes" --become' — achievable by a 2-person team in under an hour against a known host list.

Evidence: Before disabling the PackageKit service, capture the current service state and any runtime artifacts: run 'systemctl status packagekit --full --no-pager > /tmp/pk_status_$(hostname).txt', preserve '/var/log/apt/history.log' and '/var/log/dnf.log' (or '/var/log/yum.log') showing recent PackageKit-initiated installs, and dump active polkit sessions with 'pkaction --verbose 2>&1 > /tmp/pkaction_$(hostname).txt'. Capture the running process tree at time of containment: 'ps auxf > /tmp/ps_tree_$(hostname).txt'. These establish a pre-containment baseline for later comparison against unauthorized package installs or SUID modifications introduced during the exposure window.

Step 2: Detection — Query package management logs for unexpected PackageKit invocations by non-root users. On systemd-based systems, check 'journalctl -u packagekit' for authorization bypass patterns. Look for polkit policy evaluations granting org.freedesktop.packagekit.* actions to unprivileged users (audit logs via auditd, event keyword 'type=AVC' or 'type=USER_AUTH'). Monitor for new SUID binaries, unexpected cron entries, or new user accounts created post-exploitation as indicators of follow-on activity consistent with T1543.002.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, execute the following on each host: (1) 'journalctl -u packagekit --since "2026-01-01" | grep -iE "(allowed|granted|org.freedesktop.packagekit)" > /tmp/pk_journal_$(hostname).txt' to surface polkit grants to PackageKit actions; (2) 'ausearch -m USER_AUTH,AVC -ts recent | grep -i packagekit' to pull auditd events tied to polkit authorization decisions for CVE-2026-41651's bypass mechanism; (3) 'find / -perm -4000 -newer /var/lib/packagekit -ls 2>/dev/null' to identify SUID binaries created after PackageKit was first installed — a direct indicator of post-exploitation privilege persistence; (4) deploy the public Sigma rule for polkit privilege escalation (sigma/rules/linux/auditd/lnx_auditd_polkit_lpe.yml) via Chainsaw or grep-based log parsing if no SIEM is available.

Evidence: Preserve 'journalctl -u packagekit -o json > /tmp/pk_journal_json_$(hostname).txt' before any log rotation occurs — this captures PackageKit D-Bus method calls including the caller UID that should not match root (UID 0) for legitimate admin sessions. Pull '/var/log/auth.log' (Debian/Ubuntu) or '/var/log/secure' (RHEL/Rocky/Fedora) for 'su' or 'sudo' events immediately following PackageKit invocations by unprivileged UIDs, which would indicate the exploit was used to gain a root shell. Capture auditd records with 'ausearch -m EXECVE,PROCTITLE -ts recent | grep -A5 packagekitd' to reconstruct the argument chain passed to packagekitd at time of exploitation. These three sources together reconstruct the CVE-2026-41651 authorization bypass call chain.

Step 3: Eradication — Upgrade PackageKit to version 1.3.5 using your distribution's package manager. For Ubuntu: 'sudo apt update && sudo apt install packagekit'. For Fedora: 'sudo dnf upgrade packagekit'. For Debian: apply the relevant DSA update via 'sudo apt update && sudo apt upgrade packagekit'. For Rocky Linux: apply available errata via 'sudo dnf update packagekit'. Confirm the installed version post-upgrade: 'pkcon --version'.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Automate patching across your Linux fleet with Ansible: 'ansible all -m package -a "name=packagekit state=latest" --become', then validate with 'ansible all -m command -a "pkcon --version" --become' and assert output contains '1.3.5'. For air-gapped environments, download the PackageKit 1.3.5 source or distro package from the official vendor mirror, verify the SHA-256 checksum against the vendor advisory before deployment, and use 'dpkg -i' or 'rpm

-Uvh' for manual installation. If exploit artifacts (rogue SUID binaries, new accounts) were found during detection, eradicate those first by removing the binary ('rm -f /path/to/suid_binary') and locking the account ('usermod -L rogue_user') before applying the patch — patching over a live compromise without cleanup leaves persistence mechanisms intact.

Evidence: Before patching, snapshot the full installed package manifest: 'dpkg -l > /tmp/pkg_manifest_pre_patch_$(hostname).txt' or 'rpm -qa > /tmp/pkg_manifest_pre_patch_$(hostname).txt'. Also capture '/etc/passwd' and '/etc/shadow' (hashes only, for account integrity comparison), '/etc/crontab', '/var/spool/cron/crontabs/', and the output of 'find /etc/sudoers.d/ -type f -exec cat {} \;' — an attacker who successfully exploited CVE-2026-41651 to gain root would likely establish persistence via one of these vectors before patching cuts off their PackageKit escalation path. Preserving these pre-patch enables post-eradication comparison to confirm no persistence survived.

Step 4: Recovery — After patching, verify PackageKit version is 1.3.5 or later on all affected hosts. Re-enable the service only if required for operations. Review polkit rules (files under /etc/polkit-1/rules.d/ and /usr/share/polkit-1/rules.d/) for unauthorized modifications. Audit recently installed or removed packages on affected systems for the window between initial exposure (November 2014 for systems running unpatched versions) and patch application. Monitor PackageKit and polkit logs for 30 days post-remediation for anomalous authorization requests.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Validate polkit rule integrity by computing SHA-256 hashes of all files in '/etc/polkit-1/rules.d/' and '/usr/share/polkit-1/rules.d/' and comparing against a known-good baseline from a freshly imaged system of the same distro version: 'sha256sum /etc/polkit-1/rules.d/* /usr/share/polkit-1/rules.d/* > /tmp/polkit_rules_hash_$(hostname).txt'. Use 'debsums -c' (Debian/Ubuntu) or 'rpm -Va' (Fedora/Rocky) to verify integrity of all installed packages against the distro's package database — this catches any packages silently installed or tampered with via the PackageKit escalation path. For ongoing monitoring without SIEM, configure auditd with a watch rule: '-w /etc/polkit-1/rules.d/ -p wa -k polkit_mod' and '-w /usr/share/polkit-1/rules.d/ -p wa -k polkit_mod' to alert on any future unauthorized polkit rule changes.

Evidence: At recovery entry, capture the post-patch state for audit chain continuity: 'pkcon --version', 'dpkg -l packagekit' or 'rpm -q packagekit', and re-hash the polkit rules directories. Compare '/etc/passwd' and '/var/spool/cron/crontabs/' against the pre-eradication snapshots taken in Step 3 to confirm no persistence artifacts survived. Preserve all PackageKit and auditd logs from the exposure window — given the 12-year vulnerability age, systems that have been running unpatched since 2014 require a longer retrospective audit window; prioritize reviewing package install history from 'cat /var/log/apt/history.log | grep -E "^(Install|Upgrade)"' for any packages installed outside of expected maintenance windows.

Step 5: Post-Incident — This vulnerability exposes a control gap in local privilege boundary enforcement on Linux systems. Review polkit authorization policies across all Linux endpoints and servers. Assess whether the principle of least privilege is enforced for package management operations (only admins should invoke PackageKit). Consider implementing host-based IDS rules to alert on unexpected SUID/GUID file creation and unauthorized polkit grants. Update your Linux hardening baseline (referencing CIS Benchmarks for Linux distributions) to include PackageKit service state as a configuration audit item.

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 SI-2 (Flaw Remediation), NIST RA-3 (Risk Assessment), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Add PackageKit service state and version to your configuration compliance checklist using osquery: 'SELECT name, version FROM deb_packages WHERE name = "packagekit";' scheduled as a recurring osquery pack query with results alerting on version < 1.3.5 or service status = active when not operationally required. Write a Sigma rule detecting polkit grants to 'org.freedesktop.packagekit.*' actions by non-root UIDs in auditd logs (logsource: product: linux, category: auditd; keywords: USER_AUTH + packagekit + uid != 0) and run it nightly via Chainsaw against collected auditd logs. Add a YARA rule scanning for known CVE-2026-41651 PoC exploit strings or shellcode patterns in '/tmp/', '/dev/shm/', and user home directories as a weekly cron job using ClamAV with a custom YARA signature.

Evidence: For the lessons-learned record, compile: (1) the full timeline of PackageKit versions deployed per host extracted from package manager logs, establishing when each system first became vulnerable (as far back as PackageKit 1.0.2 install date); (2) a count of unique non-root UIDs that invoked PackageKit D-Bus methods during the exposure window, extracted from 'journalctl -u packagekit -o json' archives; (3) the polkit rules diff showing any unauthorized modifications found during recovery (Step 4 hash comparison results); and (4) a list of packages installed outside maintenance windows during the exposure period from 'apt/history.log' or 'dnf.log'. This evidence package supports both the post-incident report and any regulatory notification obligations if privileged data access is confirmed.

Detection Guidance

Primary detection path is PackageKit and polkit log analysis. On systemd systems, run 'journalctl -u packagekit --since today' and filter for authorization decisions involving non-root UIDs. Polkit logs authorization outcomes; look for entries granting 'org.freedesktop.packagekit.package-install' or 'org.freedesktop.packagekit.package-remove' to users outside expected admin groups. Using auditd: search for 'type=USER_AUTH' or 'type=AVC' events involving the packagekitd process. For EDR platforms, hunt for processes spawned by packagekitd with elevated privileges (UID 0) where the initiating user is non-root. Behavioral indicators consistent with post-exploitation (T1543.002): new systemd service unit files created by non-root users, unexpected entries in /etc/cron.d or /etc/sudoers.d, new accounts in /etc/passwd. Public PoC (github.com/Vozec/CVE-2026-41651) may produce characteristic process trees; signature-based detection on PoC filenames and argument patterns is an available option for endpoint security tools.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/Vozec/CVE-2026-41651`	Public proof-of-concept exploit repository for CVE-2026-41651; presence of this repository's artifacts on a host may indicate exploit staging or testing	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1548.003** — Sudo and Sudo Caching
- **T1068** — Exploitation for Privilege Escalation
- **T1543.002** — Systemd Service
- **T1548** — Abuse Elevation Control Mechanism

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-6** — Configuration Settings
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.1** — Establish an Access Granting Process
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

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(d)** — Person or Entity Authentication

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548.003	Sudo and Sudo Caching	Privilege-Escalation
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1543.002	Systemd Service	Persistence

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-pack2theroot-fla...	T3
Pack2TheRoot (CVE-2026-41651): Cross-Distro Local Privilege ...	https://github.security.telekom.com/2026/04/pack2theroot-linux-loca...	T3
Vozec/CVE-2026-41651 - GitHub	https://github.com/Vozec/CVE-2026-41651	T3
CVE-2026-41651 Common Vulnerabilities and Exposures | SUSE	https://www.suse.com/security/cve/CVE-2026-41651.html	T3
Pack2TheRoot (CVE-2026-41651): Cross-Distro Local Privilege ...	https://www.reddit.com/r/netsec/comments/1sswok7/pack2theroot_cve20...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-41651	T1

Generated 2026-04-24 18:45 UTC by TJS Security Command Center