Telekom Security

Pack2TheRoot (CVE-2026-41651): Cross-Distro Local Privilege Escalation Vulnerability

22 Apr 2026

Today we publicly disclose a high-severity vulnerability (CVSS 3.1: 8.8) - in coordination with distro maintainers - that affects multiple Linux distributions in their default installations. The Pack2TheRoot vulnerability can be exploited by any local unprivileged user to obtain root access on a vulnerable system.

The vulnerability lies in the PackageKit daemon, a cross-distro package management abstraction layer.

The vulnerability enables an unprivileged attacker to install or remove system packages without authorization. This can be exploited to gain full root access or compromise the system in other ways.

The Pack2TheRoot (CVE-2026-41651) vulnerability was discovered by Deutsche Telekom's Red Team during targeted research into local privilege escalation vectors on modern Linux systems. PackageKit as a candidate initially caught our attention when we observed that a `pkcon install` command could install a system package without requiring a password on a Fedora Workstation.

Starting in 2025, we began investigating whether this behavior could be abused to achieve arbitrary package installation. By guiding the AI-assisted research into a specific direction (using Claude Opus by Anthropic) we were able to discover an exploitable vulnerability. The finding was manually reviewed and verified before being responsibly reported to the PackageKit maintainers, who confirmed the issue and its exploitability.

Which versions and systems are vulnerable?

All PackageKit versions between `>= 1.0.2` and `<= 1.3.4` are vulnerable. Since PackageKit 1.0.2 was released over 12 years ago, this leaves a broad attack surface across Linux distributions. Exploitability has been explicitly tested and confirmed on the following distributions in default installations with `apt` and `dnf` package manager backends:

- Ubuntu Desktop 18.04 (EOL), 24.04.4 (LTS), 26.04 (LTS beta).
- Ubuntu Server 22.04 - 24.04 (LTS)
- Debian Desktop Trixie 13.4
- RockyLinux Desktop 10.1
- Fedora 43 Desktop
- Fedora 43 Server

It is reasonable to assume that all distributions that ship PackageKit with it enabled are vulnerable. Since PackageKit is an optional dependency of the Cockpit project, many servers with Cockpit installed might be vulnerable as well, including Red Hat Enterprise Linux (RHEL).

The vulnerability is fixed in PackageKit release 1.3.5 and distribution backports. Updates should be available from today 2026-04-22 12:00 CEST.

How to check if your system is vulnerable

It is not sufficient to simply `grep` through the process list, as PackageKit and Cockpit are not necessarily running as persistent processes as they can be activated on demand through D-Bus. First check if PackageKit is installed on your system and compare it with vulnerable versions, e.g.

- `dpkg -l | grep -i packagekit` or
- `rpm -qa | grep -i packagekit`

Note `grep`'s `-i` flag, as the package may be installed in camel case as `PackageKit`.

To check if the PackageKit daemon is available, run `systemctl status packagekit` or `pkmon`. If `systemctl` shows it as `loaded` or `running` or the PackageKit monitor tools show transaction output, the daemon is active and your system is potentially exploitable if unpatched. For PackageKit `< 1.3.3` test `pkmon`, for versions `>= 1.3.3` use `pkgcli monitor` to test for output.

Updated Packages

Despite of the fixed release `1.3.5`, multiple Distributions released patched packages. In the following, we link the Distros package overviews, that show Distro specific patched versions.

- Debian: https://security-tracker.debian.org/tracker/CVE-2026-41651
- Ubuntu: https://bugs.launchpad.net/bugs/cve/2026-41651
- Fedora 42 - 44: Fixed in PackageKit-1.3.4-3 https://koji.fedoraproject.org/koji/packageinfo?packageID=5206

Workaround

Disclaimer: The following workaround is provided "as is", without warranty of any kind, express or implied. Use at your own risk. Test thoroughly in your environment before deploying to production systems.

This workaround has the sideffect that GUI software centers (GNOME Software, etc.) will no longer be able to install packages. Users must use `sudo yum/dnf install` from the terminal. Package installs via `yum`/`dnf` are unaffected since they don't use PackageKit.

Systems that do not have an available patch, can be secured by deploying a PolicyKit rule file as a workaround. For polkit 0.106+ place a rulefile in `/etc/polkit-1/rules.d/49-workaround-cve-2026-41651.rules`:

```
// CVE-2026-41651 workaround: immediately deny PackageKit install actions
// without dispatching to an authentication agent.
// This prevents the transaction flag race by ensuring the polkit denial
```

```
// arrives before the scheduler's idle callback can fire.

polkit.addRule(function(action, subject) {
    if (action.id === "org.freedesktop.packagekit.package-install-untrusted" ||
        action.id === "org.freedesktop.packagekit.package-install" ||
        action.id === "org.freedesktop.packagekit.package-reinstall" ||
        action.id === "org.freedesktop.packagekit.package-downgrade" ||
        action.id === "org.freedesktop.packagekit.system-update") {

        // Allow root (uid 0) — needed for legitimate admin operations
        if (subject.uid === 0) {
            return polkit.Result.YES;
        }

        // Deny all non-root users immediately (no agent interaction)
        return polkit.Result.NO;
    }
});
```

Indicators of compromise (IOC)

Even though the vulnerability is reliably exploitable in seconds, it leaves traces that serve as a strong indicator of compromise. After successful exploitation, the PackageKit daemon hits an assertion failure and crashes. Systemd recovers the daemon on the next D-Bus invocation, preventing a denial-of-service, but the crash is observable in the system logs:

```
# journalctl --no-pager -u packagekit | grep -i emitted_finished
Apr 18 09:56:36 Rocky10 packagekitd[2082]: PackageKit:ERROR:../src/pk-transaction.
Apr 18 09:56:36 Rocky10 packagekitd[2082]: Bail out! PackageKit:ERROR:../src/pk-tr
```

Technical Details

The vulnerability is a time-of-check-time-of-use (TOCTOU) race condition in PackageKit's D-Bus transaction handling.

PackageKit and Transaction Flags

PackageKit is a D-Bus system service that runs as root and delegates authorization to polkit. When a client wants to install a package, it creates a transaction object over D-Bus and calls a method such as `InstallFiles(flags, [path])`.

The `flags` parameter is a bitfield that controls the transaction's behavior. Certain flag values (such as `SIMULATE` and `ONLY_DOWNLOAD`) cause PackageKit to skip polkit authorization entirely, because the operations they represent are considered safe: they should never modify the system.

The Root Cause

The core issue is that PackageKit's transaction handler unconditionally overwrites the cached transaction flags on every `InstallFiles` call, without verifying the transaction's current state. There is no guard ensuring the transaction is still in its initial state. A second call on the same transaction can overwrite the flags even after the transaction has already been authorized and is running.

PackageKit's state machine does have a guard against backward state transitions, but it rejects them silently. The flag overwrite happens *before* the state transition is attempted, so the corrupted flags remain in effect while the transaction continues to run.

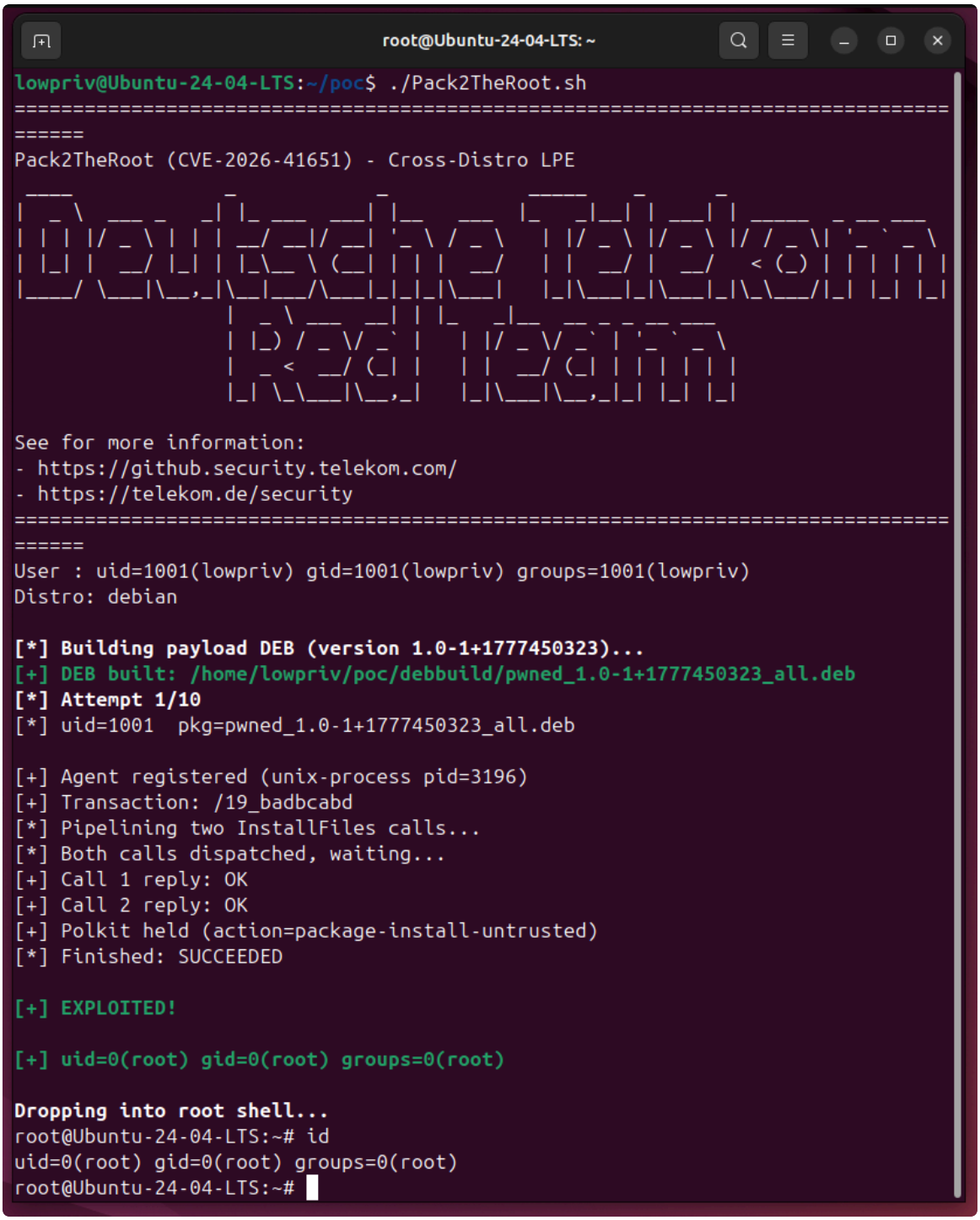
When the transaction is eventually executed, the scheduler reads the *current* value of the cached flags. If the safety flags have been stripped by a subsequent call, the backend performs a real operation instead of the originally authorized safe one.

GLib Event Loop Ordering

A key property that makes this exploitable is GLib's main loop priority system: D-Bus messages are dispatched at a higher priority than idle callbacks. The scheduler executes transactions through idle callbacks, which means any pending D-Bus message is *always* processed first. This creates a reliable window for the flag overwrite to land before the transaction actually executes.

Proof-of-Concept

We have developed a working proof-of-concept that reliably exploits this vulnerability to achieve root code execution from an unprivileged local user on default installations of various distributions. However, the PoC code is not being shared publicly at this time for obvious reasons.



Credits

A huge thank you goes to PackageKit maintainer Matthias Klumpp (@ximion), for addressing this vulnerability quickly by creating a patch and for coordinating communication with the distribution

maintainers. The vulnerability has been found and reported by Deutsche Telekom's Red Team. If you have questions regarding the vulnerability or are interested in our security offerings, including Red Team assessments, feel free to contact [loading (JS)…].

Timeline

- 2026-04-08: Private report of the vulnerability to Red Hat (through Fedora) and PackageKit project
- 2026-04-10: Acknowledgement of receipt and plausibility of the vulnerability by PackageKit maintainer
- 2026-04-13: First draft of private patch by PackageKit maintainer Matthias Klumpp (@ximion)
- 2026-04-15: Informed Canonical about the issue
- 2026-04-15: Shared patch with Red Hat and Canonical
- 2026-04-19: Privately informed distribution vendors through distros mailing list, shared patch and publication date
- 2026-04-21: Reaffirmed the publication date with distribution maintainers
- 2026-04-22: PackageKit patch release and public disclosure through oss-security mailing list and this blog post.
- 2026-04-22: Got CVE-2026-41651 assigned
- 2026-04-23: Public exploit available on GitHub
- 2026-04-29: Updated blog article with technical details and propose for workaround

Advisories

- GitHub Security Advisory GHSA-f55j-vvr9-69xv
- CVE-2026-41651