**AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION**

Centre de Réponse aux Incidents de Sécurité Informatique

**NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES**

Computer Incident Response Team

# ALERTE DE SECURITE

## *Pack2TheRoot : une faille critique d'élévation de privilèges sous Linux*

## Contenu

## I. Contexte

Une vulnérabilité majeure, baptisée **Pack2TheRoot**, vient d'être identifiée dans le démon **PackageKit**. Cette faille permettrait à un utilisateur local non privilégié d'installer ou de supprimer des paquets système, ouvrant ainsi la voie à une élévation de privilèges vers l'utilisateur root.

Répertoriée sous la référence **CVE-2026-41651**, cette faille a reçu une note de sévérité de **8,8 sur 10**. De plus, elle est restée indétectée pendant près de 12 ans au sein de PackageKit, le service d'arrière-plan chargé de la gestion des logiciels (installation, mise à jour, suppression) sur de nombreuses distributions Linux.

Bien que l'existence de cette faille soit désormais publique, les détails techniques approfondis et le code d'exploitation (PoC) ne sont pas encore disponible pour favoriser le déploiement des correctifs.

## II. Analyse de la menace

**Un défaut dans le mécanisme de gestion des paquets**

Les investigations menées par les chercheurs ont révélé que la faille réside dans la manière dont PackageKit traite les requêtes de gestion de paquets. Les chercheurs ont notamment constaté que certaines commandes, telles que pkcon install, pouvaient s'exécuter sans aucune authentification sous certaines conditions spécifiques.

En s'appuyant sur des outils d'intelligence artificielle pour approfondir leur analyse, les experts ont confirmé que ce comportement permettait de prendre le contrôle total du système.

L'étendue de cette vulnérabilité est considérable, car elle concerne une vaste gamme de systèmes d'exploitation utilisés tant par les particuliers que par les entreprises.

## III. Systèmes affectés

La vulnérabilité est présente depuis la version 1.0.2 de PackageKit (sortie en novembre 2014) et affecte toutes les itérations jusqu'à la version 1.3.4 comprise. Les distributions confirmées comme vulnérables incluent, entre autres :

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

- Fedora 43 : Desktop et Server

Cette liste n'est pas exhaustive. Toute distribution Linux utilisant PackageKit par défaut doit être considérée comme potentiellement à risque.

Face à cette menace, il est impératif d'identifier si votre parc informatique est exposé afin d'appliquer les mesures correctives nécessaires.

## IV. Diagnostic et mesures d'atténuation

Pour vérifier si votre système utilise une version vulnérable de PackageKit, vous pouvez utiliser les commandes suivantes selon votre gestionnaire de paquets :

**Sur Debian/Ubuntu** : *dpkg -l | grep -i packagekit*

**Sur RHEL/Fedora/RockyLinux** : *rpm -qa | grep -i packagekit*

Pour déterminer si le démon est actif (et donc si le vecteur d'attaque est ouvert), utilisez :

*systemctl status packagekit ou pkmon*

**Recommandation immédiate**

La mise à jour vers la version 1.3.5 de PackageKit est impérative. Assurez-vous également que tous les logiciels tiers dépendant de ce paquet ont été mis à jour vers une version sécurisée.

Enfin, même si aucune exploitation massive n'a été rapportée, certains signes ne trompent pas les administrateurs systèmes vigilants.

Les chercheurs soulignent que l'exploitation de la **CVE-2026-41651** provoque généralement un échec d'assertion (« assertion failure ») entraînant le plantage du démon PackageKit.

Même si le système (via systemd) redémarre automatiquement le service, la trace de ce plantage reste visible dans les journaux système (logs). Une surveillance accrue des logs est donc recommandée pour détecter toute tentative d'exploitation passée ou présente.

## V. Annexes

**PoC de la faille Pack2TheRoot**