AVIS DE SECURITE

Objet	**Vulnérabilité de contournement de la vérification des paquets dans APT (Debian, Ubuntu et dérivés)**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-298
TLP	WHITE

Résumé

Debian, Canonical (Ubuntu) et les développeurs d'APT ont publié le 04/11/2026 des correctifs pour la vulnérabilité CVE-2026-109518 (CVSS v4.0 : 7.7) affectant APT, le gestionnaire de paquets de Debian, d'Ubuntu et de leurs distributions dérivées. Une faiblesse de type TOCTOU (CWE-367) dans le traitement des fichiers lors de la reprise d'un téléchargement HTTP permet à un attaquant en position d'intermédiaire (y compris un miroir ou un proxy malveillant) de substituer un paquet après sa vérification et d'obtenir l'exécution de code avec les privilèges root. L'exploitation requiert un paramètre Acquire::Retries non nul, valeur par défaut (3) depuis Debian 12 et Ubuntu 22.04 LTS. Aucune exploitation active n'est signalée à ce jour.

Risque de sécurité

- Exécution de code arbitraire avec les privilèges root
- Atteinte à l'intégrité du système (installation d'un paquet non vérifié)
- Contournement de la politique de sécurité (vérification des signatures APT)
- Élévation de privilèges

Systèmes affectés

- APT (Debian, Ubuntu et distributions dérivées) : versions antérieures à 1.2.36, 1.4.12, 1.6.19, 1.8.2.4, 2.0.12, 2.2.5, 2.4.15, 2.6.2, 2.8.4, 3.0.4, 3.2.1 et 3.3.6 selon la branche, ainsi que 1.8.3 à 1.8.5
- Debian 12 (bookworm) : versions antérieures à 2.6.2 ; Debian 13 (trixie) : versions antérieures à 3.0.4 ; Debian 11 (bullseye, hors support LTS) : versions antérieures à 2.2.5
- Ubuntu 22.04 LTS, 24.04 LTS, 26.04 LTS et 26.10 : exposées dans la configuration par défaut
- Ubuntu 14.04, 16.04, 18.04 et 20.04 LTS : exposées uniquement si Acquire::Retries est non nul
- Versions corrigées Ubuntu : 2.4.15ubuntu0.1 (22.04), 2.8.4ubuntu0.1 (24.04), 3.2.1ubuntu0.1 (26.04), 3.3.3ubuntu0.1 (26.10), versions ESM pour 14.04 à 20.04

Recommandations

1. Mettre à jour le paquet apt vers la version corrigée de sa distribution en appliquant la mise à jour avec l'option -o Acquire::Retries=0 et privilégier des dépôts accessibles en HTTPS ;
2. A défaut de correctif, positionner Acquire::Retries à 0.
3. Se référer aux bulletins de sécurité des éditeurs du 04/11/2026 (DSA-6607-1, DLA-4880-1, USN-8996-1) :
   - https://ubuntu.com/security/CVE-2026-109518
   - https://ubuntu.com/blog/apt-vulnerability-fixes-available
   - https://security-tracker.debian.org/tracker/CVE-2026-109518
   - https://www.cve.org/CVERecord?id=CVE-2026-109518

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar
https://www.stcc-ssi.sn/

E-mail : sncsirt@dcssi.sn

Date de publication : 05/11/2026