DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 17-05-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans le Noyau Linux (ssh-keysign-pwn)
Réference	1473
Date de Publication	2026-05-17
Sévérité	Elevé

IMPACT :

- Vol d'identifiants et d'accès privilégiés
- Contournement des mécanismes de sécurité
- Mouvement latéral dans l'infrastructure

SYSTÉME AFFECTÉ :

- La vulnérabilité affecte la plupart des distributions Linux exécutant des kernels antérieurs au correctif publié le 14 mai 2026.

DÉSCRIPTION :

Une vulnérabilité critique a été découverte dans le noyau Linux, identifiée comme CVE-2026-46333. La faille réside dans la gestion des contrôles ptrace lors de la terminaison d'un processus privilégié. Un attaquant local peut exploiter une race condition impliquant pidfd_getfd() afin d'accéder à des file descriptors sensibles encore ouverts par un processus SUID ou root. Une exploitation réussie peut permettre le vol de clés SSH, la lecture de /etc/shadow ou l'accès à d'autres données sensibles du système.

SOLUTION :

- Appliquer les derniers correctifs du kernel.
- Faire la rotation de toutes les clés SSH, en particulier sur les systèmes critiques.
- Auditer les accès aux fichiers sensibles, tels que /etc/shadow.
- Surveiller l’utilisation suspecte de ptrace ou des appels système liés à pidfd.
- Restreindre autant que possible les accès des utilisateurs locaux, car l’exploitation nécessite une présence locale.

DOCUMENTATION :

- CVE-2026-46333

https://nvd.nist.gov/vuln/detail/CVE-2026-46333