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

Autorité Nationale de Cybersécurité

Djibouti le, 03-05-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans les distributions Linux
Réference	1465
Date de Publication	2026-05-03
Sévérité	Critique

IMPACT :

- Elévation de privilèges ;
- Injection du code arbitraire ;

SYSTÉME AFFECTÉ :

Linux kernel versions 4.14 et ultérieures, versions antérieures à 6.18.22, 6.19.12 et 7.0 (y compris les branches en fin de vie intégrant le commit 72548b093ee3).

DÉSCRIPTION :

Il s’agit d’une vulnérabilité dans l’interface **algif_aead** du noyau Linux qui traite des opérations **AEAD** via des sockets **AF_ALG**.

Linux kernel est un noyau de système d’exploitation libre utilisé par de nombreuses distributions Linux pour des environnements serveurs, postes de travail et systèmes embarqués.

Le traitement en mode **in-place** fait partager les mêmes structures de mémoire entre les buffers source et destination, ce qui place des pages du **page cache** de fichiers lisibles dans une liste de destination **inscriptible**.
L’algorithme **authencesn(hmac(sha256),cbc(aes))** effectue alors une écriture de **4 octets contrôlés** au-delà de la zone de sortie déclarée, directement dans ces pages du page cache. Cette écriture ciblée permet la **corruption en mémoire** de fichiers lisibles tels que des binaires **setuid** ou des fichiers de configuration sensibles, sans modification sur disque, ce qui contourne les contrôles d’intégrité classiques.

Elle permet à un utilisateur local non privilégié d’obtenir des droits root de manière déterministe en modifiant la vue en mémoire de fichiers critiques comme /etc/passwd ou /usr/bin/su.

SOLUTION :

Veuillez se référer au bulletin de sécurité concernant la distribution Linux utilisée.

CONTOURNEMENT PROVISOIRE :

Désactivation de l’interface algif_aead ou du support AF_ALG lorsque cela est possible.

DOCUMENTATION :

Bulletin de sécurité Red Hat:

- https://access.redhat.com/security/cve/cve-2026-31431

Bulletin de sécurité Debian:

- https://security-tracker.debian.org/tracker/CVE-2026-31431

Bulletin de sécurité Ubuntu:

- https://ubuntu.com/security/CVE-2026-31431

Bulletin de sécurité Suse:

- https://www.suse.com/security/cve/CVE-2026-31431.html