



BULLETIN DE SECURITE

Titre	Zero-day dans les distributions Linux
Numéro de Référence	63723004/26
Date de Publication	30 Avril 2026
Risque	Important
Impact	Important

Systemes affectés

- Noyau Linux (Kernel) : Toutes les versions distribuées depuis août 2017.
- Distributions majeures : Ubuntu, Debian, Red Hat Enterprise Linux (RHEL), SUSE, Amazon Linux.
- Conteneurs : Systèmes utilisant des environnements de conteneurisation (Docker, Kubernetes) partageant le même noyau.

Identificateurs externes

- CVE-2026-31431,

Bilan de la vulnérabilité

Une vulnérabilité critique de type « zero-day », baptisée "Copy Fail" (CVE-2026-31431) a été identifiée dans les différentes distributions Linux depuis août 2017. Cette vulnérabilité repose sur un défaut logique dans le sous-système cryptographique du noyau (algif_aead). L'exploitation de cette faille peut permettre à un attaquant d'injecter du code malveillant directement en mémoire et obtenir les privilèges « Root ».

Solution

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

Risque

- Elévation de privilèges ;
- Injection du code arbitraire ;

Référence

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>