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

Autorité Nationale de Cybersécurité

Djibouti le, 09-05-2026

BULLETIN ALERTES

Object	Vulnerabilites Critique sur les Systemes Linux
Réference	1467
Date de Publication	2026-05-09
Sévérité	Critique

IMPACT :

- Élévation de privilèges

SYSTÉME AFFECTÉ :

La vulnérabilité touche les noyaux Linux publiés depuis 2017. Toutes les distributions actuelles sont considérées comme vulnérables (Ubuntu, Debian, RHEL, AlmaLinux, Rocky Linux, Fedora, etc.).

DÉSCRIPTION :

Le **8 mai 2026**, les vulnérabilités **CVE-2026-43284** (surnommée *Dirty Frag*) et **CVE-2026-43500** ont été divulguées publiquement. Il s'agit d'une vulnérabilité d'**élévation de privilèges locale (LPE)** qui permet à un attaquant disposant d'un accès local (y compris via SSH) d'obtenir les droits **root** en manipulant le *page cache* du noyau Linux.

Cette vulnérabilité est particulièrement critique car elle est **déterministe** (pas de condition de course), fiable et fonctionne sur un très grand nombre de distributions Linux.

Dirty Frag est une évolution de la classe de bugs incluant *Dirty Pipe* et *Copy Fail*. Elle combine deux vulnérabilités distinctes :

- **xfrm-ESP Page-Cache Write** (CVE-2026-43284) : Permet d'écrire dans le page cache des fichiers lisibles.
- **RxRPC Page-Cache Write** (CVE-2026-43500) : Permet d'écrire dans le page cache sans créer d'espace de noms.

En combinant ces deux failles, un attaquant peut obtenir les droits root sur **presque toutes les distributions Linux majeures**, même si des mesures de mitigation partielles (comme le blacklistage de algif_aead) ont déjà été appliquées.

CONTOURNEMENT PROVISOIRE :

À ce jour (9 mai 2026), les correctifs officiels ne sont pas encore disponibles sur toutes les distributions.

Mesures de mitigation immédiates :

- Désactiver les modules du noyau suivants s'ils ne sont pas indispensables :
  - esp4
  - esp6
  - rxrpc

DOCUMENTATION :

- Bulletin d'alerte RHEL : CVE-2026-43284
- Bulletin d'alerte Debian **:** CVE-2026-43284
- Bulletin d'alerte Ubuntu : CVE-2026-43284