Journal : Et ça continue [DirtyFrag]

7 mai 2026 12

Posté par **Ambroise** le 07 mai 2026 à 23:17. **Licence CC By-SA.**
Étiquettes : **cve**, **linux**, **zero-day**, **cybersécurité**

Après CopyFail, voilà DirtyFrag… https://github.com/V4bel/dirtyfrag

Et encore une fois, il y a eu un raté sur le NDA (sauf que là, le gars dit que ce serait d'une tierce partie).

Par contre, je serais bien incapable de dire si le module impacté est nécessaire ou non à quelque chose une machine standard. Et donc je ne peux pas dire si le workaround est à faire ou non…

(8 commentaires). **Markdown** **EPUB**

Oui quand même

Posté par **cg** le 08 mai 2026 à 00:23. Évalué à 5 (+3/-0).

> Il y a trois modules listés : esp4, esp6 et rxrpc.
>
> RxRPC, je ne connais pas, mais ça semble surtout utile pour AndrewFS (AFS), un système de fichier réseau qui est, je crois, assez confidentiel.
>
> Par contre, ESP, c'est un bout d'IPSec, qui est utilisé dans *beaucoup* de technos de VPN, donc probablement présent et utile dans énormément de firewalls.
>
> Pour une machine de "particulier", ça semble sans impact de les désactiver en attendant.
>
> Vivement un exploit dans le module ipv4 directement qu'on rigole un peu :).

Répondre

[^] # Re: Oui quand même

Posté par **Voltairine** le 08 mai 2026 à 07:38. Évalué à 4 (+2/-0).
Dernière modification le 08 mai 2026 à 07:40.

> Il y a très peu de chance que ces modules soient chargés si IPsec n'est pas utilisé.
>
> Et si c'est utilisé, le contournement qui consiste décharger ces modules le rendra inopérant.
>
> Pour vérifier il suffit d'utiliser `lsmod` (en root)
>
> Comme pour l'autre PoC, attention aux tests : l'exploit sera actif tant que la mémoire cache n'est pas vidée ou la machine redémarrée.

Répondre

Ah désolé je viens de poster à ce sujet en forum et liens, je n'avais pas vu ce journal

Posté par **yinqi** le 08 mai 2026 à 11:06. Évalué à 2 (+1/-0).

> Petite question pour éviter de cela : Quelles sont les recommandations pour partager ce type d'info urgente sur LinuxFr? Est-ce Forum/Journal/Lien? (sans doute pas dépêche)
> Je pensais que Journal était plus pour des sujets de fond, n'étant pas une dépêche.

Répondre

[^] # Re: Ah désolé je viens de poster à ce sujet en forum et liens, je n'avais pas vu ce journal

Posté par **volts** (**Mastodon**) le 08 mai 2026 à 11:40.
Évalué à 2 (+0/-0).

> > Quelles sont les recommandations pour partager ce type d'info urgente sur LinuxFr? Est-ce Forum/Journal/Lien? (sans doute pas dépêche)
>
> Pour l'instant, je n'ai pas vu de recommandation formelle sur FAQ ni sur le wiki .
>
> En pratique, je privilégierais le journal pour des infos urgente. Toutefois, il est possible de faire une dépêche urgente, mais il faudra prendre un certain délai avant sa publication, le temps que l'équipe de modération valide le contenu.
>
> > Je pensais que Journal était plus pour des sujets de fond, n'étant pas une dépêche.
>
> D'après la FAQ, les journaux sont l'équivalent d'un espace de blog à disposition des inscrits. Il n'y a donc pas de contrainte explicite sur le type de contenu à mettre (sauf à ne rien faire d'illicite au regard de la loi française).

Répondre

CVE-2026-43284

Posté par **Voltairine** le 08 mai 2026 à 11:28. Évalué à 4 (+2/-0).

> Un numéro CVE a été attribué.
>
> Le suivi pour :
>
> - Debian
> - Redhat
> - Ubuntu
>
> Le correctif publié pour le noyau.

Répondre

[^] # Re: CVE-2026-43284

Posté par **volts** (**Mastodon**) le 08 mai 2026 à 11:47.
Évalué à 2 (+0/-0).

> Ça me retourne une erreur 404 pour le lien de Ubuntu 🫠 .

Répondre

comme d'habitude ?

Posté par **dovik** (**site web personnel**) le 08 mai 2026 à 11:35.
Évalué à 2 (+0/-0).

> On est d'accord que toutes ses failles nécessitent un accès local ?

> Il me semble que, depuis toujours, il faut considérer un accès local sur une machine comme une machine compromise.
>
> Du coup : c'est intéressant, mais peut-être pas nécessaire de communiquer dessus comme si c'était la fin du monde à chaque fois ?

Répondre

[^] # Re: comme d'habitude ?

Posté par **Glandos** le 08 mai 2026 à 11:41. Évalué à 2 (+0/-0).

> Pas forcément compromise, non. 
> Exemple : j'administre des machines qui enregistrent des images de vidéosurveillance. Des techniciens ont le droit de se connecter dessus, avec des droits réduits, pour observer les journaux et redémarrer les services. Mais pas installer des nouveaux paquets ou arrêter la machine.
>
> Ceci étant dit, le fait que ça nécessite un accès local réduit fortement la sévérité, en effet.

Répondre

Envoyer un commentaire

Suivre le flux des commentaires

Note : les commentaires appartiennent à celles et ceux qui les ont postés. Nous n'en sommes pas responsables.

Revenir en haut de page

Derniers commentaires

- C'est bien mais
- Re: CVE-2026-43284
- Re: Yes
- Re: comme d'habitu…
- Re: Ah désolé je vie…
- comme d'habitude ?
- CVE-2026-43284
- Re: apps gtk ou qt
- Doublon avec un jo…
- Ah désolé je viens d…
- Déjà un journal avec…
- Données perso

Étiquettes (tags) populaires

- intelligence_artificielle
- rétro-informatique
- grands_modèles_de…
- cybersécurité
- merdification
- souveraineté_numer…
- france
- administration_fran…
- sortie_version
- linux
- jeu_vidéo
- capitalisme_de_surv…

Sites amis

- Agenda du Libre
- April
- Éditions D-BookeR
- Éditions Diamond
- Éditions Eyrolles
- Éditions ENI
- En Vente Libre
- Framasoft
- La Quadrature du Net
- Lea-Linux
- Open Source Initiative
- Imprimerie Grafik Plus

À propos de LinuxFr.org

- Mentions légales
- Faire un don
- L'équipe de LinuxFr.…
- Informations sur le s…
- Aide / Foire aux que…
- Suivi des suggestion…
- Wiki du site
- Règles de modération
- Statistiques
- API pour le dévelop…
- Code source du site
- Plan du site