AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

La vulnérabilité zero-day Dirty Frag qui menace l'intégrité du noyau Linux

Contenu

I. Contexte

Une nouvelle faille de sécurité majeure, baptisée Dirty Frag, a été révélée par les chercheurs en cybersécurité. Cette exploitation de type "zero-day" permet à un utilisateur local malveillant d'obtenir des privilèges root (super-utilisateur) sur la majorité des distributions Linux via une commande unique. Introduite il y a environ neuf ans dans l'interface de l'algorithme cryptographique *algif_aead* du noyau, cette vulnérabilité représente un risque immédiat pour l'intégrité des systèmes.

II. Analyse technique et mécanisme d'attaque

Contrairement à d'autres failles reposant sur des conditions de concurrence instables, Dirty Frag se distingue par sa fiabilité exceptionnelle. Elle fonctionne en enchaînant deux vulnérabilités distinctes d'écriture dans le cache de pages (Page-Cache Write) : celle liée à xfrm-ESP et celle liée à RxRPC.

Bien que Dirty Frag appartienne à la même famille que les célèbres failles Dirty Pipe et Copy Fail, elle cible une structure de données différente du noyau : le champ de fragmentation (fragment field). Selon les chercheurs à l'origine de la découverte, l'exploit est déterministe : il ne provoque pas de "kernel panic" en cas d'échec et affiche un taux de réussite très élevé.

Cette dangerosité technique explique l'impact étendu de la faille sur l'écosystème Linux.

III. Systèmes affectés

L'alerte concerne un large spectre de distributions professionnelles et communautaires, notamment :

- Ubuntu
- Red Hat Enterprise Linux (RHEL)
- CentOS Stream / AlmaLinux
- openSUSE Tumbleweed
- Fedora

La divulgation publique a été effectuée le 7 mai 2026, en conséquence, les vulnérabilités sont désormais identifiées sous les références suivantes :

CVE-2026-43284 (faille xfrm-ESP)

CVE-2026-43500 (faille RxRPC)

Face à l'absence de correctifs immédiats pour toutes les distributions, des mesures d'atténuation d'urgence doivent être envisagées.

IV. Recommandations

En l'attente des mises à jour officielles des éditeurs, les administrateurs système peuvent désactiver les modules vulnérables. Cette manipulation interrompra les services VPN IPsec et les systèmes de fichiers distribués AFS.

Pour sécuriser vos systèmes, exécutez la commande suivante afin de neutraliser les modules esp4, esp6 et rxrpc :

sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' > /etc/modprobe.d/dirtyfrag.conf; rmmod esp4 esp6 rxrpc 2>/dev/null; true"

Surveillez étroitement les dépôts de sécurité de vos distributions respectives et appliquez les correctifs dès leur disponibilité.

V. Conclusion

L'apparition de Dirty Frag survient alors que les mainteneurs luttent encore contre Copy Fail, une autre vulnérabilité de privilèges root activement exploitée. Ces incidents successifs, incluant la faille Pack2TheRoot corrigée en avril, soulignent une persistance des vecteurs d'attaque ciblant les composants profonds du système Linux.