GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPP 9108 Port-Vila, Vanuatu
Tél: (678) 33380

08 octobre 2025

Avis 101 : Vulnérabilité d'écriture hors limites dans le tas du noyau Linux

Date de publication : 06 octobre 2025
Degré d'impact : ÉLEVÉ/ CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN par l'intermédiaire du CERT Vanuatu (CERTVU)), publie la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

Objet de l'alerte

CVE-2021-22555 est une **écriture hors limites** dans le tas dans l'implémentation Netfilter du noyau Linux (fichier net/netfilter/x_tables.c) qui a été découverte en 2021. La faille existe dans la gestion de setsockopt() (IPT_SO_SET_REPLACE / IP6T_SO_SET_REPLACE) et permet la corruption de la mémoire de tas lorsqu'elle est exploitée dans certaines conditions, entraînant une élévation de privilèges ou un déni de service (crash système).

Systemes concernés

La faille affecte les noyaux Linux depuis la version v2.6.19-rc1 et a été corrigée dans le noyau principal 5.12 (et reportée vers un ensemble de branches stables). Tout noyau plus ancien que les niveaux de rétroportage corrigés est considéré comme potentiellement vulnérable, sauf indication contraire du fournisseur.

Implication

Une exploitation réussie peut entraîner **une élévation des privilèges locaux au niveau racine**, **l'exécution de code noyau ou un déni de service** (crash système). Étant donné qu'il existe des PdC capables de contourner les techniques d'atténuation classiques, il est considéré comme une élévation de privilèges du noyau à fort impact.

Cela permet à un attaquant d'obtenir des privilèges ou de provoquer un déni de service (via une corruption de la mémoire de tas) via l'espace nom utilisateur.

Mesures d'atténuation

Le CERTVU recommande les mesures suivantes :

1. Correctif : appliquez les mises à jour du noyau du fournisseur. Mettez à niveau le noyau Linux et les paquets du système d'exploitation vers une version qui contient le correctif officiel.
2. Désactivez les espaces de noms d'utilisateurs non privilégiés, renforcez la sécurité des comptes locaux (supprimez ou verrouillez les comptes locaux non utilisés).
3. Appliquez le renforcement de l'hôte : réduisez le nombre de services sur lesquels des utilisateurs non fiables peuvent exécuter du code (par exemple, limitez l'accès SSH, désactivez les commandes interactives pour les comptes de service) et séparez les charges de travail afin que les utilisateurs non fiables ne puissent pas exécuter de code sur des machines qui doivent rester non corrigées.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2021-22555
3. https://github.com/google/security-research/security/advisories/GHSA-xxx5-8mvq-3528