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
Tel: (678) 33380

08 octobre 2025

Avis 103 : Vulnérabilité d'élévation de privilèges dans Microsoft Windows

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-2021-43226 est une vulnérabilité d'élévation de privilèges (EoP) dans le pilote Windows Common Log File System (CLFS) qui peut permettre à un attaquant local d'obtenir des privilèges plus élevés sur un système vulnérable.

Systemes concernés

Versions affectées:

Elle affecte plusieurs clients et serveurs Windows (Microsoft l'a identifiée comme une vulnérabilité du pilote Windows CLFS révélée en décembre 2021 et corrigée dans le cadre de la mise à jour Microsoft de décembre 2021 (voir le lien ci-dessous).

https://isc.sans.edu/diary/28132

Implication

Un attaquant doit déjà disposer d'un certain niveau d'accès pour exécuter du code ou des commandes sur la cible. En exploitant la faille du pilote CLFS, l'attaquant peut augmenter ses privilèges à un niveau supérieur (par exemple, SYSTEM), ce qui lui permet d'effectuer d'autres actions sur le système hôte.

Mesures d’atténuation

Le CERTVU recommande les mesures suivantes :

Appliquez les mises à jour de correctifs Microsoft.

Surveillez également les activités suspectes d'élévation des privilèges locaux.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2021-43226
3. https://isc.sans.edu/diary/28132