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

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

28 avril 2026

Avis 133 : Vulnérabilité de lecture hors limites dans Microsoft Windows (CVE-2023-36424)

Date de publication : 13 avril 2026
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publie l'avis suivant.

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

Objet de l'alerte

CVE-2023-36424 est une vulnérabilité d'élévation de privilèges (EoP) de haute gravité (CVSS 7.8) dans Microsoft Windows. Elle affecte le pilote Windows Common Log File System (CLFS), un composant central du noyau chargé de la gestion de la journalisation transactionnelle.

Systèmes concernés

La vulnérabilité affecte un large éventail de plateformes Microsoft Windows, incluant :

- Windows 10 (plusieurs versions : 1507 → 22H2)
- Windows 11 (21H2, 22H2, 23H2)
- Windows Server 2008 / 2012 / 2016 / 2019 / 2022

Étant donné que CLFS est un composant central du noyau, la plupart des systèmes Windows modernes sont potentiellement concernés s'ils ne sont pas corrigés.

Implications

Il s'agit d'une vulnérabilité d'élévation de privilèges locale (LPE), ce qui signifie que les attaquants doivent déjà avoir accès au système (par exemple, via un logiciel malveillant ou des identifiants compromis).

Chaîne d'exploitation typique :

1. **Accès initial**
   - L'attaquant obtient un point d'appui sur le système (par exemple, via du phishing, une infection par logiciel malveillant ou un autre exploit).
2. **Déclenchement de la faille CLFS**
   - Une entrée ou un objet spécialement conçu est transmis au pilote CLFS.
3. **Exploitation d'un défaut de gestion de la mémoire**
   - Le pilote valide ou lit incorrectement la mémoire, entraînant une condition de dépassement de limites (out-of-bounds).
4. **Élévation de privilèges**
   - L'attaquant parvient à élever ses privilèges, passant d'un utilisateur standard à un accès de niveau SYSTEM.

L'exploitation réussie de cette vulnérabilité peut permettre aux attaquants de :

- Obtenir des privilèges de niveau SYSTEM.
- Exécuter du code arbitraire avec un contrôle total.
- Installer des logiciels malveillants ou des portes dérobées persistantes.
- Accéder à des données sensibles, les modifier ou les supprimer.
- Désactiver les contrôles de sécurité.
- Utiliser le système pour des mouvements latéraux au sein d'un réseau.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

1. Appliquer les mises à jour de sécurité Microsoft (critique)

- Installer immédiatement les dernières mises à jour de sécurité de Windows (Patch Tuesday de novembre 2023 et ultérieures).
- S'assurer que tous les terminaux sont entièrement corrigés et régulièrement mis à jour.

2. Restreindre l'accès initial

- Réduire les privilèges des utilisateurs (appliquer le principe du moindre privilège).
- Restreindre la possibilité d'exécuter du code non fiable.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2023-36424
3. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36424

.