AVIS DE SECURITE

Objet	Vulnérabilité importante d'élévation de privilèges dans le noyau sécurisé (Secure Kernel Mode) de Microsoft Windows 11
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-204
TLP	WHITE

Résumé

Microsoft a publié le 14 septembre 2026 un correctif pour une vulnérabilité de type double libération de mémoire (double free, CWE-415) dans le mode noyau sécurisé (Secure Kernel Mode) de Windows 11 version 26H1 (CVE-2026-85921, CVSS 8.2). Un attaquant local déjà authentifié à faible privilège peut exploiter cette faille pour élever ses privilèges jusqu'au niveau système. Microsoft indique que la vulnérabilité n'est pas divulguée publiquement, qu'aucune exploitation active n'a été constatée à ce jour, et que l'exploitation est jugée peu probable.

Risque de sécurité

- Élévation de privilèges locale jusqu'au niveau système (CVE-2026-85921, CVSS 8.2, double libération de mémoire — CWE-415)
- Contournement des mécanismes d'isolation du noyau sécurisé (VBS/HVCI)
- Compromission complète du poste ou serveur Windows affecté à partir d'un accès local à faible privilège

Systèmes affectés

- Windows 11 version 26H1 pour systèmes x64, versions antérieures à 10.0.28000.2956
- Windows 11 version 26H1 pour systèmes ARM64, versions antérieures à 10.0.28000.2956

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 14 septembre 2026 :

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85921