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

20 janvier 2026

Avis 117 : Vulnérabilité de divulgation d'informations dans Microsoft Windows

Date de publication : 13 janvier 2026
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-2026-20805 est une vulnérabilité de sécurité dans le gestionnaire de fenêtres du bureau (GFB) de Microsoft Windows, à travers laquelle un attaquant disposant d'un accès local à un ordinateur affecté, peut divulguer des informations sensibles (données en mémoire) censées être sécurisées. Il s'agit d'une faille de divulgation d'informations, dont l'exploitation active a été confirmée avant la publication d'un correctif.

Systèmes concernés

Cette vulnérabilité affecte plusieurs versions de Microsoft Windows exécutant le GFB, y compris un large éventail d'éditions Windows 10, Windows 11 et Windows Server antérieures aux mises à jour de sécurité de janvier/février 2026.

Implication

Pour exploiter cette faille :

- L'attaquant doit disposer d'un accès authentifié local (c'est-à-dire d'un compte sur la machine).
- Il peut exploiter la manière dont le GFB fonctionne pour divulguer des adresses mémoire et d'autres données sensibles.
- Ces informations peuvent permettre de contourner des mécanismes de protection tels que la randomisation de l'espace mémoire (REM), facilitant ainsi l'enchaînement de vulnérabilités supplémentaires pour l'élévation des privilèges ou la compromission du système.

Mesures d'atténuation

Le CERTVU recommande les mesures suivantes :

1. Appliquez les mises à jour de sécurité Microsoft du *Patch Tuesday* de janvier/février 2026 (installez les mises à jour cumulatives pertinentes pour vos versions Windows).
2. Déployez les correctifs de toute urgence.
3. Surveillez les activités suspectes, telles que les activités de GFB anormales ou les élévations de privilèges locaux.
4. Suivez les meilleures pratiques générales, telles que les comptes à privilèges minimaux et les défenses de terminaux à jour, afin de limiter l'utilisation latérale des informations divulguées.

Références

.

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-20805