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

13 janvier 2026

Avis 111 : Vulnérabilité dans Microsoft Windows Race Condition

Date de publication : 12 novembre 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-2025-62215 – Il s'agit d'une condition de concurrence (vulnérabilité liée à une synchronisation incorrecte présente dans le noyau Windows). Plus précisément, plusieurs menaces ou processus accèdent à une ressource partagée du noyau sans synchronisation appropriée, ce qui permet à un attaquant local d'augmenter ses privilèges.

Systèmes concernés

Versions affectées :

- Les versions prises en charge de Windows 10, Windows 11 et Windows Server (y compris les versions récentes) sont concernées.
- Les systèmes exécutant des versions du noyau jusqu'à (mais à l'exclusion de) certaines versions corrigées sont vulnérables.

- Comme il s'agit d'une faille au niveau du noyau, tout poste de travail ou serveur sur lequel un utilisateur peut exécuter du code localement (ou qui est déjà compromis dans une certaine mesure) est exposé à un risque d'élévation de privilèges.

Implication

Les attaquants peuvent exploiter cette vulnérabilité par les manières suivantes (vecteur d'attaque) :

- L'attaquant doit disposer d'un certain niveau d'exécution de code local ou d'accès pour pouvoir exploiter la vulnérabilité (par exemple, un compte utilisateur ou un processus). La vulnérabilité n'est pas entièrement à distance sans accès.
- L'attaquant déclenche la condition de concurrence en exécutant ou en orchestrant une opération simultanée sur la ressource partagée du noyau afin de provoquer une corruption de la mémoire ou un échec de synchronisation. Cela peut alors conduire à une escalade des privilèges.
- Une fois ses privilèges élevés, l'attaquant peut prendre le contrôle total du système, contourner les contrôles des applications, désactiver les fonctionnalités de sécurité, installer des portes dérobées persistantes, se déplacer latéralement ou utiliser l'hôte compromis comme passerelle.

Mesures d'atténuation

Le CERTVU recommande les mesures suivantes :

Application immédiate des correctifs – Appliquez le correctif Microsoft Patch Tuesday de novembre 2025.

Si les correctifs ne peuvent pas être déployés immédiatement :

- Restreignez les comptes utilisateurs : veillez à ce que les privilèges locaux des utilisateurs soient réduits au minimum.
- Surveillez les systèmes afin de détecter tout signe d'élévation anormale des privilèges locaux.
- Restreignez ou désactivez les mécanismes qui permettent aux utilisateurs de charger ou d'exécuter localement du code non fiable – Cela réduit la surface d'attaque.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-62215