

**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



**GOVERNEMENT 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 131 : Vulnérabilité de suivi de lien dans Microsoft Windows (CVE-2025-60710).**

**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-2025-60710** est une vulnérabilité de haute gravité permettant une élévation de privilèges (CVSS 7.8) affectant les systèmes Microsoft Windows. La faille se situe dans le processus hôte pour les tâches Windows, en raison d'une résolution incorrecte des liens avant l'accès aux fichiers.

## **Systemes concernés**

Versions affectées :

- Microsoft Windows 11 (notamment les versions 24H2 et 25H2) ;
- Les systèmes exécutant des versions vulnérables du processus hôte pour les tâches Windows.

# Implications

Il s'agit d'une vulnérabilité d'élévation de privilèges locaux (LPE), ce qui signifie que les attaquants doivent d'abord disposer d'un certain niveau d'accès au système.

## Chaîne d'exploitation typique :

1. **Accès initial**
  - L'attaquant obtient un accès de bas niveau (par exemple via un logiciel malveillant, du phishing ou une autre vulnérabilité).
2. **Création d'un lien ou d'une référence de fichier malveillant**
  - L'attaquant crée un lien symbolique ou un chemin de fichier manipulé pointant vers une ressource système sensible.
3. **Déclenchement du processus vulnérable**
  - Le processus hôte des tâches Windows suit incorrectement le lien malveillant lors des opérations sur les fichiers.
4. **Élévation de privilèges**
  - L'attaquant redirige les opérations vers des fichiers ou des emplacements protégés, ce qui lui permet d'obtenir des privilèges plus élevés, jusqu'au niveau SYSTEM.

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

- Élever leurs privilèges au niveau SYSTEM ou administrateur.
- Exécuter du code arbitraire avec des permissions élevées.
- Accéder à ou modifier des fichiers systèmes sensibles.
- Désactiver des contrôles ou mécanismes de sécurité.
- Établir une persistance et se déplacer latéralement au sein d'un réseau.

En raison de son potentiel d'élévation de privilèges, cette vulnérabilité est fréquemment intégrée dans des attaques multi-étapes, intervenant après une compromission initiale.

# 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 Windows corrigeant CVE-2025-60710.
- S'assurer que les systèmes sont mis à jour au-delà des versions vulnérables (par exemple, versions corrigées après les publications de 2025).

---

## 2. Limiter l'accès et les privilèges locaux

- Appliquer le principe du moindre privilège pour les utilisateurs et les applications.
- Restreindre les droits administratifs et surveiller les tentatives d'élévation de privilèges.

## Références

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2025-60710>
3. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710>