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

1 June 2026

Avis 143 : Vulnérabilité de dépassement de tampon dans Microsoft Windows

Date de publication : 20 mai 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-2008-4250 est une vulnérabilité critique d'exécution de code à distance (RCE) dans le service serveur de Microsoft Windows. La faille est causée par une requête RPC mal gérée, entraînant un dépassement de tampon basé sur la pile.

Cette vulnérabilité est devenue largement connue à travers son exploitation par le ver **Conficker** et est associée au bulletin de sécurité Bulletin MS08-067

Systèmes concernés

La vulnérabilité affecte les anciens systèmes Microsoft Windows, y compris :

- Windows 2000
- Windows XP
- Windows Vista

- Windows Server 2003
- Windows Server 2008 (certaines configurations)

Parce que vCenter gère de manière centralisée l'infrastructure virtuelle, il constitue une cible de grande valeur.

Implications

Cette vulnérabilité est **« wormable »,** ce qui veut dire qu'elle peut se propager automatiquement à travers les réseaux sans interaction de l'utilisateur.

Chaîne d'exploitation typique :

1. **Analyse de la cible**
   - Les attaquants recherchent des systèmes exposant les services SMB/RPC (TCP 445).
2. **Envoi d'une requête RPC malveillante**
   - Un paquet réseau spécialement conçu est envoyé au service serveur de Windows.
3. **Déclenchement du dépassement de tampon**
   - Un contrôle incorrect des limites provoque un dépassement de pile en mémoire.
4. **Exécution de code arbitraire**
   - L'attaquant exécute du code malveillant avec les privilèges SYSTEM.
5. **Propagation automatisée**
   - Le logiciel malveillant peut analyser d'autres systèmes vulnérables et se propager de lui-même.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

Appliquer les mises à jour de sécurité Microsoft (Critique)

- Installer immédiatement la mise à jour de sécurité MS08-067 sur les systèmes vulnérables.
- S'assurer que tous les systèmes Windows sont entièrement corrigés.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2008-4250
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
4. https://support.microsoft.com/en-us/topic/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execution-ac7878fc-be69-7143-472d-2507a179cd15