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

28 octobre 2025

Avis 104 : Vulnérabilité d'écriture hors limites dans Microsoft Windows

Date de publication : 6 octobre 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publient 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 administrateurs de systèmes.

Objet de l'alerte

La vulnérabilité **CVE-2013-3918** correspond à une faille de type écriture hors limites entraînant une corruption de mémoire au sein du contrôle ActiveX **InformationCardSigninHelper** (icardie.dll), utilisé par Internet Explorer. Cette vulnérabilité peut être exploitée à distance lorsqu'un utilisateur accède à une page web malveillante, ce qui peut conduire à une exécution arbitraire de code sur le système ciblé.

Systèmes concernés

Versions affectées :

Les systèmes Windows intégrant le contrôle ActiveX icardie.dll comprennent :

- Windows XP SP2/SP3,
- Windows Server 2003 SP2,

- Windows Vista SP2,
- Windows Server 2008 SP2/R2 SP1,
- Windows 7 SP1, Windows 8/8.1,
- Windows RT
- Ainsi que les versions correspondantes de Windows Server 2012 (voir le bulletin du fournisseur pour la correspondance CPE). Les systèmes non corrigés depuis novembre 2013 restent vulnérables.

Implications

Un attaquant réussissant à exploiter cette vulnérabilité pourrait obtenir les mêmes droits que l'utilisateur actuel. Le produit concerné peut être en fin de vie ou en fin de support. Il est recommandé aux utilisateurs de cesser d'utiliser ce produit.

Mesures d'atténuation

CERTVU recommande :

D'appliquer immédiatement les mises à jour de sécurité fournies par Microsoft.

Dans l'éventualité où l'application immédiate des correctifs ne serait pas possible, il est conseillé de désactiver ou de restreindre le contrôle ActiveX concerné (voir la configuration du kill-bit via les stratégies de groupe, conformément aux recommandations du bulletin de sécurité Microsoft).

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2013-3918
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-090