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 105 : Vulnérabilité d'exécution de code à distance 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-2011-3402** correspond à une faille d'exécution de code à distance dans le moteur **d'analyse des polices TrueType** (win32k.sys). Elle permet l'exécution de code en mode noyau via des données de police spécialement conçues, contenues dans une page web ou un document Office.

Systèmes concernés

Les versions de Windows concernées incluent :

- Windows XP (SP2/SP3),
- Windows Server 2003 (SP2),
- Windows Vista (SP2),
- Windows Server 2008 (SP2 / R2),

- Windows 7 (Gold / SP1) and
- Ainsi que les versions serveurs correspondantes supportées en 2011. Autrement dit, les systèmes n'ayant pas reçu la mise à jour MS11-087 restent vulnérables.

Implications

Cette vulnérabilité permet à des attaquants distants d'exécuter du code arbitraire en exploitant des données de police malveillantes intégrées dans un document Word ou une page web. Elle a notamment été utilisée en conditions réelles en novembre 2011 par le malware Duqu, et est également connue sous le nom de « vulnérabilité d'analyse des polices TrueType ».

Mesures d'atténuation

CERTVU recommande :

D'appliquer immédiatement les mises à jour de sécurité fournies par Microsoft.
D'installer la mise à jour de sécurité Microsoft MS11-087 (13 décembre 2011) qui corrige la vulnérabilité CVE-2011-3402.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2011-3402
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-087
4. https://exploitshop.wordpress.com/2012/01/18/ms11-087-aka-duqu-vulnerability-in-windows-kernel-mode-drivers-could-allow-remote-code-execution/