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 avril 2026

Avis 130 : Chargement non sécurisé de bibliothèques dans Microsoft Visual Basic for Applications (CVE-2012-1854)

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-2012-1854 est une vulnérabilité critique permettant l'exécution de code à distance dans Microsoft Windows. Elle affecte le composant Microsoft XML Core Services (MSXML), utilisé notamment par Internet Explorer et d'autres applications.

La faille est causée par une gestion incorrecte des objets en mémoire (use-after-free / corruption de mémoire) lors du traitement de contenu web spécialement conçu. Cela permet à des attaquants de corrompre la mémoire et d'exécuter du code arbitraire.

Systèmes concernés

Versions affectées :

La vulnérabilité concerne d'anciennes plateformes Microsoft, notamment :

- Microsoft Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

Ainsi que les composants associés :

- Microsoft XML Core Services (MSXML), versions 3.0, 4.0, 5.0 et 6.0
- Internet Explorer (diverses versions à l'époque).

Remarque : Ces systèmes sont désormais **en fin de vie (End-of-Life, EOL)** et ne reçoivent plus de mises à jour de sécurité, ce qui accroît le risque en cas d'utilisation.

Implications

Chaîne d'attaque typique :

1. **Page web malveillante ou diffusion de contenu**
   - Les attaquants hébergent un site web spécialement conçu ou injectent du code malveillant dans des sites légitimes.
2. **Interaction de l'utilisateur**
   - La victime visite la page web malveillante en utilisant Internet Explorer ou une application utilisant MSXML.
3. **Déclenchement de la vulnérabilité**
   - . Le contenu malveillant provoque une mauvaise gestion des objets en mémoire par MSXML.
4. **Corruption de la mémoire (use-after-free)**
   - L'application accède à une zone mémoire déjà libérée, permettant l'exécution de données contrôlées par l'attaquant.
5. **Exécution de code à distance**
   - L'attaquant exécute du code arbitraire dans le contexte de l'utilisateur connecté.

Vecteurs d'attaque :

- Sites web malveillants.
- Sites légitimes compromis (drive-by downloads).
- Emails de phishing contenant des liens malveillants.

L'exploitation réussie de la vulnérabilité **CVE-2012-1854** peut permettre à des attaquants de :

- Exécuter du code arbitraire sur le système cible.
- Installer des logiciels malveillants ou des logiciels espions.
- Voler des informations sensibles.
- Prendre le contrôle total du système affecté (si l'utilisateur dispose de privilèges administrateur).
- Utiliser le système comme point d'appui pour compromettre davantage le réseau.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

1. Appliquer les mises à jour de sécurité Microsoft

- Installer les mises à jour fournies dans le bulletin de sécurité Microsoft MS12-043 (juin 2012).
- S'assurer que tous les composants MSXML sont mis à jour vers des versions corrigées.

2. Mettre à niveau ou remplacer les systèmes hérités (critique)
3. Utiliser des navigateurs modernes

- Éviter les anciennes versions d'Internet Explorer.
- Privilégier des navigateurs modernes disposant de contrôles de sécurité renforcés et de mécanismes de sandboxing.

4. Appliquer le principe du moindre privilège

- Exploiter des systèmes avec des comptes utilisateurs sans privilèges administrateur afin de réduire l'impact en cas d'attaque.

5. Protection du réseau et des terminaux.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2012-1854
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-043
4. https://support.microsoft.com/en-us/topic/ms12-043-description-of-the-security-update-for-xml-core-services-5-0-when-it-is-installed-together-with-office-2007-office-compatibility-pack-office-word-viewer-expression-web-or-expression-web-2-august-14-2012-b67932c4-637f-f75e-4784-083e82818920

.