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

SPP 9108 Port-Vila, Vanuatu
Tel: (678) 33380

8 octobre 2025

Avis 102 : Vulnérabilité de corruption de mémoire non initialisée dans Microsoft Internet Explorer

Date de publication : 06 octobre 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN par l'intermédiaire du CERT Vanuatu (CERTVU)), publie la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

Objet de l'alerte

CVE-2010-3962 est une vulnérabilité de type « use-after-free » / corruption de mémoire non initialisée dans Microsoft Internet Explorer (IE) qui a été divulguée en novembre 2010. Cette vulnérabilité permet à une page Web spécialement conçue de déclencher un traitement incorrect d'un objet (via des séquences de jetons CSS et l'attribut clip), entraînant une corruption de la mémoire et une exécution potentielle de code à distance dans le même contexte que l'utilisateur qui consulte la page.

Systemes concernés

Versions affectées:

Internet Explorer 6, 7 et 8 (sur les plateformes Windows concernées à cette date).

Implication

Les attaquants malveillants peuvent exploiter cette faille ou ce vecteur d'attaque par les moyens suivants :

- Attaque à distance du côté client : un attaquant héberge ou injecte une page Web spécialement conçue, que les victimes chargent à l'aide d'une version vulnérable d'IE (Internet Explorer). Il déclenche alors l'exploitation de la condition « use-after-free » et parvient à corrompre la mémoire, ce qui peut être enchaîné pour exécuter un code arbitraire. Un attaquant pourrait également exploiter cette faille dans des e-mails HTML ou des documents Word dans certaines chaînes d'attaque.
- « Exploit in the Wild » : cette vulnérabilité a été activement exploitée en novembre 2010 et reste une cible courante pour les kits d'exploitation Web obscurs et les attaques ciblées côté client.

Mesures d'atténuation

Le CERTVU recommande les mesures suivantes :

1. Appliquez immédiatement le correctif – appliquez la mise à jour de sécurité Microsoft mentionnée dans MS10-090 .

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2010-3962
3. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-090