**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 145 : Vulnérabilité de type Use-After-Free dans Microsoft Internet Explorer

**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-2010-0249** est une vulnérabilité critique d'exécution de code à distance (RCE) dans Microsoft Internet Explorer. La faille est causée par une vulnérabilité de corruption de mémoire, utilisation après libération (use-after-free) dans la manière dont Internet Explorer gère certains objets HTML et feuilles de style en cascade (CSS).

Lorsqu'un utilisateur visite une page web malveillante spécialement conçue, Internet Explorer peut accéder de manière incorrecte à une mémoire déjà libérée, permettant ainsi à un attaquant d'exécuter du code arbitraire sur le système de la victime.

# Systèmes concernés

La vulnérabilité affecte :

- **Microsoft Internet Explorer 6, 7, et 8**

- Les systèmes Microsoft Windows pris en charge à l'époque incluent :
    - Windows XP
    - Windows Vista
    - Windows 7
    - Windows Server 2003/2008

# Implications

Chaîne d'exploitation typique :

1. **Préparation d'un site web malveillant**
    - L'attaquant crée une page contenant du HTML/CSS et du JavaScript spécialement conçus.
2. **Leurres pour attirer la victime sur le site**
    - Méthodes de livraison possibles :
        - courriels de phishing
        - liens envoyés par messagerie instantanée
        - sites légitimes compromis
3. **Déclenchement de la corruption mémoire**
    - Internet Explorer gère incorrectement certains objets et accède à une mémoire invalide.
4. **Exploitation de type Use-After-Free**
    - L'attaquant manipule la mémoire libérée pour rediriger le flux d'exécution.
5. **Exécution de code à distance**
    - Du code malveillant s'exécute avec les privilèges de l'utilisateur connecté.

# Mesures d'atténuation

CERTVU recommande les mesures suivantes :

Appliquer les mises à jour de sécurité Microsoft (Critique).

# Références


1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2010-0249