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 106 : Vulnérabilité d'exécution de code à distance affectant plusieurs produits Mozilla

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-2010-3765** concerne une faille **d'exécution de code à distance** présente dans plusieurs produits Mozilla (Firefox, SeaMonkey, Thunderbird). Elle résulte d'un dépassement de tampon mémoire dans le tas, déclenché par l'utilisation conjointe de *document.write* et d'opérations d'insertion dans le DOM. Cette vulnérabilité a fait l'objet d'exploitations actives entre octobre et novembre 2010.

Systèmes concernés

Versions affectées :

- Firefox, versions **3.5.x** jusqu'à la **3.5.14** et **3.6.x** jusqu'à la **3.6.11** — corrigée dans les versions **Firefox 3.5.15** et **3.6.12**.
- SeaMonkey, corrigée à partir de la version **2.0.10**.

- Thunderbird, corrigée dans les versions **3.0.10** and **3.1.6**.
  (Toutes les installations utilisant encore des versions antérieures à ces correctifs demeurent vulnérables.)

Implications

À distance, côté client : du JavaScript malveillant présent sur une page web (ou du contenu de type web dans des flux RSS/extensions lorsque l'exécution JS est activée) exploite un suivi d'index incorrect dans `nsCSSFrameConstructor::ContentAppended`, combiné aux interactions entre `appendChild et document.write`, pour provoquer une corruption du tas (heap). Le code malveillant télécharge ensuite et exécute des charges utiles (par exemple Belmoo / backdoor dans les incidents observés). Les exploits ont été diffusés via des pages malveillantes et des kits d'exploitation en circulation.

Cela permet à des attaquants distants d'exécuter du code arbitraire en exploitant des vecteurs liés à la fonction nsCSSFrameConstructor::ContentAppended. Cette exploitation entraîne une corruption de la mémoire, comme cela a été observé dans des attaques actives en octobre 2010.

Mesures d'atténuation

CERTVU recommande :

1. D'appliquer les correctifs immédiatement – Mettre à jour vers les versions corrigées des produits concernés.
2. Si la mise à jour des postes n'est pas possible, désactiver JavaScript pour les contenus non fiables, bloquer les sites non approuvés via un proxy ou un filtrage d'URL, et restreindre l'utilisation des flux RSS ou des extensions exécutant du contenu web.
3. De renforcer la sécurité des postes en maintenant à jour les signatures antivirus et EDR.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2010-3765
3. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:JS/CVE-2010-3765