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
Tél: (678) 33380

18 décembre 2025

Avis 116 : Vulnérabilité WebKit « use-after-free » affectant plusieurs produits Apple

Date de publication : 15 décembre 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-2025-43529 est une vulnérabilité de type utilisation après libération (*use-after-free*) dans WebKit, le moteur de navigation utilisé par **Safari** et tous les navigateurs basés sur WebKit sur les plateformes Apple. Une utilisation après libération se produit lorsque le logiciel continue à référencer une mémoire qui a déjà été libérée, ce qui peut entraîner une corruption de la mémoire et l'exécution de code à distance (RCE) lors du traitement de contenu spécialement conçu. Cette vulnérabilité est activement exploitée dans la nature.

Systèmes concernés

La vulnérabilité affecte les appareils Apple et les composants du système d'exploitation utilisant WebKit, notamment :

- **iOS et iPadOS** (antérieurs à la version 26.2/18.7.3).
- **macOS Tahoe** (antérieur à la version 26.2).
- **tvOS, watchOS, visionOS** (antérieurs à la version 26.2).
- **Navigateur Safari** sur ces plateformes.

En pratique, cela signifie que de nombreux iPhone, iPad, Mac, Apple TV, Apple Watch et appareils Vision Pro fonctionnant avec des versions antérieures du système d'exploitation sont vulnérables.

Implication

Les attaquants peuvent exploiter cette vulnérabilité par les manières suivantes (vecteur d'attaque) :

Un attaquant crée un code **HTML/CSS/JavaScript malveillant** qui déclenche l'utilisation après libération dans WebKit pendant que le navigateur de la victime affiche la page. Cela provoque une corruption contrôlée de la mémoire, permettant à l'attaquant **d'exécuter du code arbitraire** dans le contexte du processus du navigateur.

• **Impact** : exploité avec succès, cela peut entraîner :

- **Exécution de code à distance (RCE)** — l'attaquant exécute du code sur l'appareil en tant qu'utilisateur du navigateur.
- **Abus de privilèges** s'il est combiné à d'autres failles.
- Compromission supplémentaire de l'appareil via des exploits en chaîne.

Mesures d’atténuation

Le CERTVU recommande les mesures suivantes :

Appliquez immédiatement le correctif : installez les mises à jour de sécurité publiées par Apple (elles corrigent la vulnérabilité CVE-2025-43529) :

- **iOS et iPadOS :** 18.7.3, 26.2 ou version ultérieure.
- **macOS Tahoe** : 26.2 ou version ultérieure.
- **tvOS, watchOS, visionOS :** 26.2 ou version ultérieure.
- **Safari :** 26.2 ou version ultérieure.

Références

1. https://threatprotect.qualys.com/2025/12/16/apple-warns-of-zero-day-vulnerability-exploited-in-attack-cve-2025-43529/
2. https://support.apple.com/en-us/125886
3. https://support.apple.com/en-us/125885

.