



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans les produits Apple
Numéro de Référence	45712301/24
Date de Publication	23 Janvier 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- iPhone 8, iPhone 8 Plus, iPhone X, iPad 5e génération, iPad Pro 9,7 pouces et iPad Pro 12,9 pouces 1re génération.
- iPhone XS et versions ultérieures, iPad Pro 12,9 pouces 2e génération et versions ultérieures, iPad Pro 10,5 pouces, iPad Pro 11 pouces 1re génération et versions ultérieures, iPad Air 3e génération et versions ultérieures, iPad 6e génération et versions ultérieures, et iPad mini 5e génération et versions ultérieures.
- Macs exécutant macOS Monterey et versions ultérieures
- Apple TV HD et Apple TV 4K (tous les modèles)

Identificateurs externes

- CVE-2024-23222

Bilan de la vulnérabilité

Apple a publié des mises à jour de sécurité pour corriger une vulnérabilité critique de type "zero-day" (CVE-2024-23222) dans ses produits. Cette vulnérabilité est activement exploitée. Une exploitation réussie de la vulnérabilité WebKit pourrait permettre à un attaquant d'exécuter un code malveillant arbitraire sur des appareils fonctionnant avec des versions vulnérables d'iOS, macOS et tvOS après l'ouverture d'une page web malveillante.

Solution

Veillez se référer au bulletin de sécurité Apple du 22 janvier 2024, afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire à distance

Référence

Bulletin de sécurité Apple du 22 janvier 2024:

- <https://support.apple.com/en-us/HT214061>