



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Apple
Numéro de Référence	43962209/23
Date de Publication	22 Septembre 2023
Risque	Critique
Impact	Critique

Systemes affectés

- Macs fonctionnant sous macOS Ventura
- iPhone 8 et versions ultérieures
- iPad Pro (tous les modèles)
- iPad Air 3e génération et versions ultérieures
- iPad 5e génération et versions ultérieures
- iPad mini 5e génération et versions ultérieures
- Apple Watch Series 4 et versions ultérieures

Identificateurs externes

- CVE-2023-41991, CVE-2023-41992, CVE-2023-41993

Bilan de la vulnérabilité

Apple a publié des mises à jour de sécurité pour corriger trois vulnérabilités critiques de type "zero-day" (CVE-2023-41991, CVE-2023-41992, et CVE-2023-41993). Ces vulnérabilités sont activement exploitées.

Les vulnérabilités sont les suivantes :

- CVE-2023-41991 - Une vulnérabilité de validation de certificat dans le Security Framework qui pourrait permettre à un attaquant de contourner la détection de signature en utilisant des applications malveillantes.
- CVE-2023-41992 - Une vulnérabilité dans le Kernel Framework qui pourrait permettre à un attaquant local d'élever ses privilèges.
- CVE-2023-41993 - Une vulnérabilité dans le moteur Webkit qui pourrait être exploitée à l'aide d'une page web malicieusement conçue, entraînant l'exécution de code arbitraire sur les produits concernés.

Il est conseillé aux utilisateurs des produits concernés d'appliquer les mises à jour le plus tôt possible.

Solution :

Veillez se référer aux bulletins de sécurité Apple du 21 Septembre 2023.

Risque :

- Exécution du code arbitraire à distance,
- Elévation de privilèges,
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Apple du 21 Septembre 2023:

- <https://support.apple.com/en-us/HT213926>
- <https://support.apple.com/en-us/HT213930>
- <https://support.apple.com/en-us/HT213931>