



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits d'Apple
Numéro de Référence	41981905/23
Date de Publication	19 Mai 2023
Risque	Important
Impact	Critique

Systemes affectés

- iOS versions antérieures à 16.5
- iPadOS versions antérieures à 16.5
- Apple Safari versions antérieures à 16.5
- Apple watchOS versions antérieures à 9.5
- Apple tvOS version antérieures à 16.5
- iOS versions antérieures à 15.7.6
- iPadOS versions antérieures à 15.7.6
- macOS Big Sur versions antérieures à 11.7.7
- macOS Ventura versions antérieures à 13.4
- macOS Monterey versions antérieures à 12.6.6

Identificateurs externes

CVE-2023-23532	CVE-2023-23535	CVE-2023-27930	CVE-2023-27940	CVE-2023-27945
CVE-2023-28181	CVE-2023-28191	CVE-2023-28202	CVE-2023-28204	CVE-2023-32352
CVE-2023-32354	CVE-2023-32355	CVE-2023-32357	CVE-2023-32360	CVE-2023-32363
CVE-2023-32365	CVE-2023-32367	CVE-2023-32368	CVE-2023-32369	CVE-2023-32371
CVE-2023-32372	CVE-2023-32373	CVE-2023-32375	CVE-2023-32376	CVE-2023-32380
CVE-2023-32382	CVE-2023-32384	CVE-2023-32385	CVE-2023-32386	CVE-2023-32387
CVE-2023-32388	CVE-2023-32389	CVE-2023-32390	CVE-2023-32391	CVE-2023-32392
CVE-2023-32394	CVE-2023-32395	CVE-2023-32397	CVE-2023-32398	CVE-2023-32399
CVE-2023-32400	CVE-2023-32402	CVE-2023-32403	CVE-2023-32404	CVE-2023-32405
CVE-2023-32407	CVE-2023-32408	CVE-2023-32409	CVE-2023-32410	CVE-2023-32411

CVE-2023-32412 CVE-2023-32413 CVE-2023-32414 CVE-2023-32415 CVE-2023-32417
CVE-2023-32419 CVE-2023-32420 CVE-2023-32422 CVE-2023-32423

Bilan de la vulnérabilité

Apple annonce la correction de plusieurs vulnérabilités critiques affectant ses produits susmentionnés. Trois de ces vulnérabilités identifiées par « CVE-2023-32409 », « CVE-2023-28204 » et CVE-2023-32373 sont des « Zero-days » Activement exploités et peuvent permettre à un attaquant distant d'exécuter du code arbitraire de contourner des mesures de sécurité ou d'accéder à des données confidentielles.

Solution

Veillez se référer aux bulletins de sécurité de l'éditeur pour l'obtention du correctif.

Risque

- Exécution de code arbitraire
- Contournement de mesures de sécurité
- Accès à des données confidentielles

Références

Bulletins de sécurité d'Apple :

- <https://support.apple.com/kb/HT213762>
- <https://support.apple.com/kb/HT213764>
- <https://support.apple.com/kb/HT213761>
- <https://support.apple.com/kb/HT213757>
- <https://support.apple.com/kb/HT213765>
- <https://support.apple.com/kb/HT213760>
- <https://support.apple.com/kb/HT213758>
- <https://support.apple.com/kb/HT213759>