



Faille de sécurité critique dans plusieurs produits Apple

Date de l'alerte : 17 février 2022

Risques

Espionnage, vol, voire destruction, de vos données suite à la prise de contrôle à distance de vos équipements concernés.

Description

Une **faille de sécurité critique** a été corrigée dans les **systèmes d'exploitation d'Apple** : **iOS** (pour téléphones iPhone et baladeurs iPod touch), **iPadOS** (pour tablettes iPad), **macOS Monterey** (pour ordinateurs Mac, MacBook et iMac) et **Safari** (navigateur Internet).

L'exploitation de cette faille de sécurité peut permettre la prise de contrôle à distance des équipements concernés et le vol, voire la destruction, d'informations par des cybercriminels.

Selon Apple, **des attaques en cours exploitant cette vulnérabilité auraient été constatées.**

Systèmes concernés

- **iOS** et **iPadOS**, versions antérieures à 15.3.1
- **macOS Monterey**, versions antérieures à 12.2.1
- **Safari**, versions antérieures à 15.3

De nombreux appareils Apple sont concernés car la vulnérabilité affecte les modèles anciens ainsi que les plus récents.

Mesure à prendre

Mettre à jour au plus vite les équipements concernés avec les correctifs de sécurité mis à disposition par Apple.

Procédure

- Pour iOS, iPadOS : <https://support.apple.com/fr-fr/HT204204>
- Pour macOS Monterey : <https://support.apple.com/fr-fr/HT201541>
- Pour Safari : <https://support.apple.com/fr-fr/HT204416>

Besoin d'assistance ?

Vous pouvez trouver sur [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures : [Ici](#).

Références

- ANSSI / CERT-FR : <https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-137/>
- CVE-2022-22620

Aller plus loin avec [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) :
[Pourquoi et comment bien gérer ses mises à jour ?](#)

