



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans les produits Apple
<b>Numéro de Référence</b>	46411103/24
<b>Date de Publication</b>	11 Mars 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- macOS Monterey versions antérieures à 12.7.4
- macOS Ventura versions antérieures à 13.6.5
- macOS Sonoma versions antérieures à 14.4
- Safari versions antérieures à 17.4

### Identificateurs externes

- CVE-2022-42816 CVE-2022-48554 CVE-2023-28826 CVE-2023-42853 CVE-2023-48795 CVE-2023-51384 CVE-2023-51385 CVE-2024-0258 CVE-2024-23201 CVE-2024-23203 CVE-2024-23204 CVE-2024-23205 CVE-2024-23216 CVE-2024-23217 CVE-2024-23218 CVE-2024-23225 CVE-2024-23226 CVE-2024-23227 CVE-2024-23230 CVE-2024-23231 CVE-2024-23232 CVE-2024-23233 CVE-2024-23234 CVE-2024-23235 CVE-2024-23238 CVE-2024-23239 CVE-2024-23241 CVE-2024-23242 CVE-2024-23244 CVE-2024-23245 CVE-2024-23246 CVE-2024-23247 CVE-2024-23248 CVE-2024-23249 CVE-2024-23250 CVE-2024-23252 CVE-2024-23253 CVE-2024-23254 CVE-2024-23255 CVE-2024-23257 CVE-2024-23258 CVE-2024-23259 CVE-2024-23260 CVE-2024-23263 CVE-2024-23264 CVE-2024-23265 CVE-2024-23266 CVE-2024-23267 CVE-2024-23268 CVE-2024-23269 CVE-2024-23270 CVE-2024-23272 CVE-2024-23273 CVE-2024-23274 CVE-2024-23275 CVE-2024-23276 CVE-2024-23277 CVE-2024-23278 CVE-2024-23279 CVE-2024-23280 CVE-2024-23281 CVE-2024-23283 CVE-2024-23284 CVE-2024-23285 CVE-2024-23286 CVE-2024-23287 CVE-2024-23288 CVE-2024-23289 CVE-2024-23290 CVE-2024-23291 CVE-2024-23292 CVE-2024-23293 CVE-2024-23294 CVE-2024-23296

### Bilan de la vulnérabilité

Apple a publié des mises à jour de sécurité d'urgence pour corriger plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant de causer un déni de service, de réussir une élévation de privilèges, de porter atteinte à la confidentialité des données et d'exécuter du code arbitraire à distance. Se-

Ion Apple, il est possible que les deux failles «CVE-2024-23225 et CVE-2024-23296 » aient déjà été exploitées.

## **Solution**

Veillez se référer au bulletin de sécurité Apple du 07 Mars 2024 pour plus d'information.

## **Risque**

- Atteinte à la confidentialité des données
- Elévation de privilèges
- Exécution du code arbitraire à distance
- Dénier de service

## **Annexe**

Bulletin de sécurité Aruba du 07 Mars 2024:

- <https://support.apple.com/en-us/HT214083>
- <https://support.apple.com/en-us/HT214084>
- <https://support.apple.com/en-us/HT214085>
- <https://support.apple.com/en-us/HT214089>