|  |
| --- |
| **Multiple Vulnérabilités dans les produits Apple** |
| **CVE-2024-27280** **CVE-2025-24088** **CVE-2025-24133** **CVE-2025-24197** **CVE-2025-30468** **CVE-2025-31254** **CVE-2025-31255** **CVE-2025-31259** **CVE-2025-31268** **CVE-2025-31269** **CVE-2025-31270** **CVE-2025-31271** **CVE-2025-40909** **CVE-2025-43190** **CVE-2025-43203** **CVE-2025-43204** **CVE-2025-43207** **CVE-2025-43208** **CVE-2025-43231** **CVE-2025-43262** **CVE-2025-43263** **CVE-2025-43272** **CVE-2025-43273** **CVE-2025-43277** **CVE-2025-43279** **CVE-2025-43283** **CVE-2025-43285** **CVE-2025-43286** **CVE-2025-43287** **CVE-2025-43291** **CVE-2025-43292** **CVE-2025-43293** **CVE-2025-43294** **CVE-2025-43295** **CVE-2025-43297** **CVE-2025-43298** **CVE-2025-43299** **CVE-2025-43300** **CVE-2025-43301** **CVE-2025-43302** **CVE-2025-43303** **CVE-2025-43304** **CVE-2025-43305** **CVE-2025-43307** **CVE-2025-43308** **CVE-2025-43310** **CVE-2025-43311** **CVE-2025-43312** **CVE-2025-43314** **CVE-2025-43315** **CVE-2025-43316** **CVE-2025-43317** **CVE-2025-43318** **CVE-2025-43319** **CVE-2025-43321** **CVE-2025-43325** **CVE-2025-43326** **CVE-2025-43327** **CVE-2025-43328** **CVE-2025-43329** **CVE-2025-43330** **CVE-2025-43331** **CVE-2025-43332** **CVE-2025-43333** **CVE-2025-43337** **CVE-2025-43340** **CVE-2025-43341** **CVE-2025-43342** **CVE-2025-43343** **CVE-2025-43344** **CVE-2025-43346** **CVE-2025-43347** **CVE-2025-43349** **CVE-2025-43353** **CVE-2025-43354** **CVE-2025-43355** **CVE-2025-43356** **CVE-2025-43357** **CVE-2025-43358** **CVE-2025-43359** **CVE-2025-43362** **CVE-2025-43366** **CVE-2025-43367** **CVE-2025-43368** **CVE-2025-43369** **CVE-2025-43370** **CVE-2025-43371** **CVE-2025-43372** **CVE-2025-43375** **CVE-2025-48384** **CVE-2025-6965** |
| **DXC MA CTI Advisory**  16/09/2025 |

Overview

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVE** | **Description** | **CVSS Score** | **Risque** | **Exploit** | **Délai de traitement** |
| **CVE-2024-27280 CVE-2025-24088 CVE-2025-24133 CVE-2025-24197 CVE-2025-30468 CVE-2025-31254 CVE-2025-31255 CVE-2025-31259 CVE-2025-31268 CVE-2025-31269 CVE-2025-31270 CVE-2025-31271 CVE-2025-40909 CVE-2025-43190 CVE-2025-43203 CVE-2025-43204 CVE-2025-43207 CVE-2025-43208 CVE-2025-43231 CVE-2025-43262 CVE-2025-43263 CVE-2025-43272 CVE-2025-43273 CVE-2025-43277 CVE-2025-43279 CVE-2025-43283 CVE-2025-43285 CVE-2025-43286 CVE-2025-43287 CVE-2025-43291 CVE-2025-43292 CVE-2025-43293 CVE-2025-43294 CVE-2025-43295 CVE-2025-43297 CVE-2025-43298 CVE-2025-43299 CVE-2025-43300 CVE-2025-43301 CVE-2025-43302 CVE-2025-43303 CVE-2025-43304 CVE-2025-43305 CVE-2025-43307 CVE-2025-43308 CVE-2025-43310 CVE-2025-43311 CVE-2025-43312 CVE-2025-43314 CVE-2025-43315 CVE-2025-43316 CVE-2025-43317 CVE-2025-43318 CVE-2025-43319 CVE-2025-43321 CVE-2025-43325 CVE-2025-43326 CVE-2025-43327 CVE-2025-43328 CVE-2025-43329 CVE-2025-43330 CVE-2025-43331 CVE-2025-43332 CVE-2025-43333 CVE-2025-43337 CVE-2025-43340 CVE-2025-43341 CVE-2025-43342 CVE-2025-43343 CVE-2025-43344 CVE-2025-43346 CVE-2025-43347 CVE-2025-43349 CVE-2025-43353 CVE-2025-43354 CVE-2025-43355 CVE-2025-43356 CVE-2025-43357 CVE-2025-43358 CVE-2025-43359 CVE-2025-43362 CVE-2025-43366 CVE-2025-43367 CVE-2025-43368 CVE-2025-43369 CVE-2025-43370 CVE-2025-43371 CVE-2025-43372 CVE-2025-43375 CVE-2025-48384 CVE-2025-6965** | De multiples vulnérabilités ont été découvertes dans les produits Apple. Elles permettent à un attaquant d'exécuter du code arbitraire à distance, de porter atteinte à la confidentialité des données, de réussir une élévation de privilèges, de causer un déni de service et de contourner la politique de sécurité. | **2.8 - 9.8** | **Exécution de code arbitraire - Atteinte à la confidentialité des données - Contournement de la politique de sécurité - Déni de service - Élévation de privilèges** | **NON** | **2 Jr** |

Produits affectés

|  |
| --- |
| · watchOS versions antérieures à 26 · visionOS versions antérieures à 26 · tvOS versions antérieures à 26 · macOS Tahoe versions antérieures à 26 · macOS Sonoma versions antérieures à **14.8** · macOS Sequoia versions antérieures à **15.7** · iPadOS versions antérieures à 26 · iPadOS versions **18.x** antérieures à **18.7** · iPadOS versions **16.x** antérieures à **16.7.12** · iPadOS versions **15.x** antérieures à **15.8.5** · iOS versions antérieures à 26 · iOS versions **18.x** antérieures à **18.7** · iOS versions **16.x** antérieures à **16.7.12** · iOS versions **15.x** antérieures à **15.8.5** · Xcode versions antérieures à 26 · Safari versions antérieures à 26 |

Mitigations & Workarounds

Mise à jour des produits Apple par les versions suivantes:  
 Ø ➢ watchOS version 26 ou ultérieure  
 Ø ➢ visionOS version 26 ou ultérieure  
 Ø ➢ tvOS version 26 ou ultérieure  
 Ø ➢ macOS Tahoe version 26 ou ultérieure  
 Ø ➢ macOS Sonoma version **14.8** ou ultérieure  
 Ø ➢ macOS Sequoia version **15.7** ou ultérieure  
 Ø ➢ iPadOS version 26 ou ultérieure  
 Ø ➢ iPadOS versions **18.x** version **18.7** ou ultérieure  
 Ø ➢ iPadOS versions **16.x** version **16.7.12** ou ultérieure  
 Ø ➢ iPadOS versions **15.x** version **15.8.5** ou ultérieure  
 Ø ➢ iOS version 26 ou ultérieure  
 Ø ➢ iOS versions **18.x** version **18.7** ou ultérieure  
 Ø ➢ iOS versions **16.x** version **16.7.12** ou ultérieure  
 Ø ➢ iOS versions **15.x** version **15.8.5** ou ultérieure  
 Ø ➢ Xcode version 26 ou ultérieure  
 Ø ➢ Safari version 26 ou ultérieure

DXC MA Cyber Threat Intelligence Assessment

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Références).

Références :

|  |
| --- |
|  |
| https://support.apple.com/en-us/125108 https://support.apple.com/en-us/125109 https://support.apple.com/en-us/125110 https://support.apple.com/en-us/125111 https://support.apple.com/en-us/125112 https://support.apple.com/en-us/125113 https://support.apple.com/en-us/125114 https://support.apple.com/en-us/125115 https://support.apple.com/en-us/125116 https://support.apple.com/en-us/125117 https://support.apple.com/en-us/125141 https://support.apple.com/en-us/125142 |