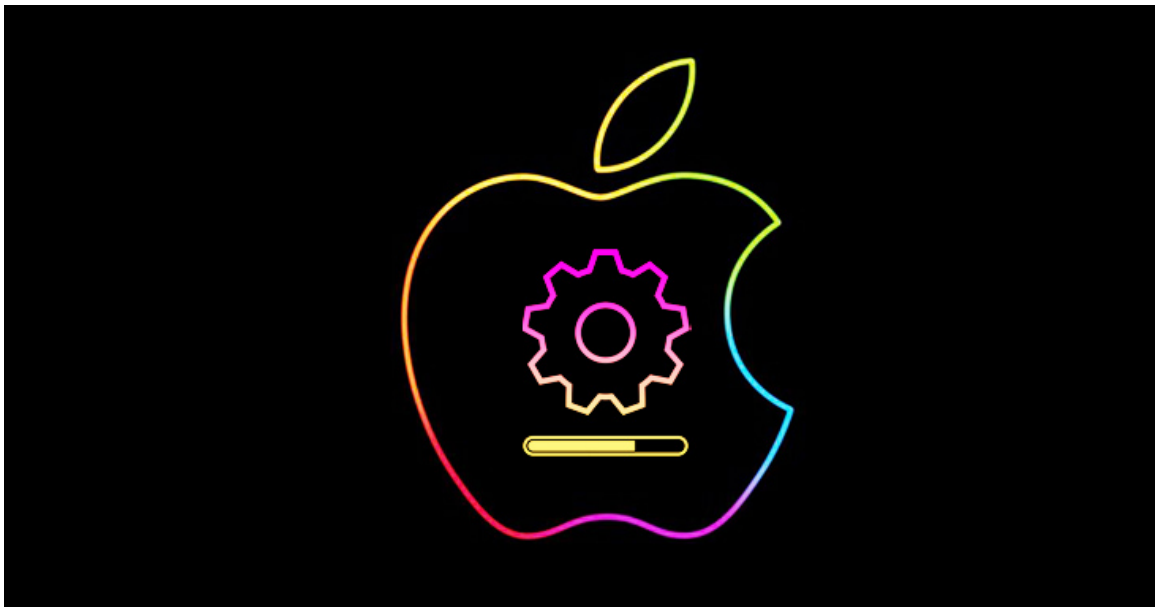
Apple déploie des correctifs urgents pour les failles zero-day affectant les iPhones, iPads et Mac

Vulnérabilités ou Attaques ou Exploits ou Failles Zero-Day:
Les attaques zero-day, aussi appelées exploits zero-day, sont des tentatives réussies par les cybercriminels de trouver et d'exploiter des vulnérabilités inconnues dans un logiciel.

Il n'existe pas de solution miracle qui empêche complètement l'exploitation des vulnérabilités 'zero day'.
Les pare-feux surveillent le trafic entrant et sortant de votre réseau, ce qui réduit les connexions non autorisées au fil du temps.

L'un des meilleurs moyens d'éviter une vulnérabilité zero-day est de disposer d'un pare-feu solide et actualisé, et de tenir à jour votre antivirus de manière optimale.

Les vulnérabilités logicielles zero-day doivent être résolues le jour même par les développeurs



Apple a déployé des mises à jour de sécurité pour iOS, iPadOS, macOS, tvOS, watchOS et Safari pour corriger plusieurs vulnérabilités de sécurité, dont une a activement exploité le bogue zero-day dans la nature.

Suivi comme **CVE-2023-38606**, le défaut réside dans le noyau et permet à une application malveillante de modifier potentiellement l'état sensible du noyau.
La société a déclaré qu'elle avait été traitée avec une meilleure gestion de l'État.

« Apple est au courant d'un rapport selon lequel ce problème pourrait avoir été activement exploité contre des versions d'iOS publiées avant iOS 15.7.1 », a noté le géant de la technologie dans son avis.

Il convient de noter que CVE-2023-38606 est la troisième vulnérabilité de sécurité découverte dans le cadre de l'opération Triangulation, une campagne sophistiquée de cyber-espionnage mobile ciblant les appareils iOS depuis 2019 à l'aide d'une chaîne d'exploitation sans clic.
Les deux autres zero-days, CVE-2023-32434 et CVE-2023-32435, ont été corrigés par Apple le mois dernier.

Les chercheurs de Kaspersky Valentin Pashkov, Mikhail Vinogradov, Georgy Kucherin, Leonid Bezvershenko et Boris Larin ont été crédités d'avoir découvert et signalé la faille.

Les mises à jour sont disponibles pour les périphériques et systèmes d'exploitation suivants :

- iOS 16.6 et iPadOS 16.6 - iPhone 8 et modèles ultérieurs, iPad Pro (tous les modèles), iPad Air 3e génération et modèles ultérieurs, iPad 5e génération et modèles ultérieurs et iPad mini 5e génération et modèles ultérieurs

- iOS 15.7.8 et iPadOS 15.7.8 - iPhone 6s (tous les modèles), iPhone 7 (tous les modèles), iPhone SE (1re génération), iPad Air 2, iPad mini (4e génération) et iPod touch (7e génération)
- macOS Ventura 13.5, macOS Monterey 12.6.8 et macOS Big Sur 11.7.9
- tvOS 16.6 - Apple TV 4K (tous les modèles) et Apple TV HD, et
- watchOS 9.6 - Apple Watch Series 4 et versions ultérieures

Avec la dernière série de correctifs, Apple a résolu un total de 11 zero-days impactant son logiciel depuis le début de 2023.
Cela arrive également deux semaines après que la société a publié des correctifs d'urgence pour un bogue activement exploité dans WebKit qui pourrait conduire à l'exécution arbitraire de code (CVE-2023-37450).

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230725
"C'est ensemble qu'on avance"