El miércoles, Apple adaptó y trasladó a versiones anteriores correcciones para una falla de seguridad en iOS, iPadOS y macOS Sonoma, después de descubrirse que estaba siendo utilizada como parte del kit de exploits Coruna.

La vulnerabilidad, identificada como CVE-2023-43010, corresponde a un problema no especificado en WebKit que podría provocar corrupción de memoria al procesar contenido web malicioso especialmente diseñado. El fabricante del iPhone indicó que el problema fue solucionado mediante un manejo mejorado del proceso.

"Esta corrección vinculada con el kit de exploits Coruna se lanzó en iOS 17.2 el 11 de diciembre de 2023," señaló Apple en un aviso de seguridad. *"Esta actualización lleva esa solución a dispositivos que no pueden actualizar a la versión más reciente de iOS."*

Las correcciones para CVE-2023-43010 fueron publicadas originalmente por Apple en las siguientes versiones:

- iOS 17.2 y iPadOS 17.2
- macOS Sonoma 14.2
- Safari 17.2

La ronda más reciente de actualizaciones ahora también las incorpora en versiones anteriores de iOS y iPadOS:

- iOS 15.8.7 y iPadOS 15.8.7 – iPhone 6s (todos los modelos), iPhone 7 (todos los modelos), iPhone SE (1.ª generación), iPad Air 2, iPad mini (4.ª generación) y iPod touch (7.ª generación)
- iOS 16.7.15 y iPadOS 16.7.15 – iPhone 8, iPhone 8 Plus, iPhone X, iPad (5.ª generación), iPad Pro de 9.7 pulgadas y iPad Pro de 12.9 pulgadas (1.ª generación)
- Además, iOS 15.8.7 y iPadOS 15.8.7 incluyen parches para otras tres vulnerabilidades relacionadas con el kit de exploits Coruna:

- CVE-2023-43000 (corregida originalmente en iOS 16.6, lanzado el 24 de julio de 2023)

– Un problema de tipo use-after-free en WebKit que podría causar corrupción de memoria al procesar contenido web malicioso especialmente diseñado.
- CVE-2023-41974 (corregida originalmente en iOS 17, lanzado el 18 de septiembre de 2023) – Una falla de tipo use-after-free en el kernel que podría permitir que una aplicación ejecute código arbitrario con privilegios del kernel.
- CVE-2024-23222 (corregida originalmente en iOS 17.3, lanzado el 22 de enero de 2024) – Un problema de confusión de tipos en WebKit que podría permitir la ejecución de código arbitrario al procesar contenido web malicioso especialmente diseñado.

Los detalles sobre Coruna surgieron a principios de este mes después de que Google indicara que el kit de exploits incluye 23 exploits organizados en cinco cadenas diseñadas para atacar modelos de iPhone que ejecutan versiones de iOS entre la 13.0 y la 17.2.1. La empresa iVerify, que rastrea el marco de malware que utiliza este kit bajo el nombre CryptoWaters, afirmó que presenta similitudes con marcos de explotación desarrollados previamente por actores de amenazas vinculados al gobierno de Estados Unidos.

Este desarrollo se produce en medio de especulaciones de que Coruna probablemente fue creado por el contratista militar estadounidense L3Harris Technologies y que posteriormente habría sido transferido al intermediario ruso de exploits Operation Zero por Peter Williams, exdirector general de la empresa, quien el mes pasado fue condenado a más de siete años de prisión por vender varios exploits a cambio de dinero.

Un aspecto llamativo de Coruna es el uso de dos exploits (CVE-2023-32434 y CVE-2023-38606) que previamente fueron utilizados como zero-days en una campaña conocida como Operation Triangulation dirigida contra usuarios en Rusia durante 2023. La compañía Kaspersky declaró a The Hacker News que cualquier equipo con suficientes capacidades técnicas podría desarrollar sus propios exploits, dado que ambas vulnerabilidades cuentan con implementaciones disponibles públicamente.

"A pesar de nuestra investigación exhaustiva, no hemos podido atribuir Operation Triangulation a ningún grupo APT conocido ni a una empresa de desarrollo de exploits," explicó Boris Larin, investigador principal de seguridad en Kaspersky GReAT.

“Para ser precisos: ni Google ni iVerify afirman en sus investigaciones publicadas que Coruna reutilice el código de Triangulation. Lo que identifican es que dos exploits de Coruna — Photon y Gallium — apuntan a las mismas vulnerabilidades. Esa es una diferencia importante. En nuestra opinión, la atribución no puede basarse únicamente en el hecho de que se exploten esas vulnerabilidades.”