Apple ha lanzado una nueva serie de parches de seguridad para abordar tres vulnerabilidades zero-day activamente explotadas que afectan a iOS, iPadOS, macOS, watchOS y Safari, lo que eleva a 16 el total de vulnerabilidades zero-day descubiertas en su software este año.

La lista de vulnerabilidades de seguridad es la siguiente:

- CVE-2023-41991: Un problema de validación de certificados en el marco de seguridad que podría permitir que una aplicación maliciosa evite la validación de firmas.
- CVE-2023-41992: Una falla de seguridad en el Kernel que podría permitir a un atacante local aumentar sus privilegios.
- CVE-2023-41993: Una falla en WebKit que podría dar como resultado la ejecución de código arbitrario al procesar contenido web especialmente diseñado.

Apple no proporcionó detalles adicionales, excepto que reconoció que el *«problema puede haber sido aprovechado activamente en versiones de iOS anteriores a iOS 16.7».*

Las actualizaciones están disponibles para los siguientes dispositivos y sistemas operativos:

- iOS 16.7 y iPadOS 16.7: iPhone 8 en adelante, iPad Pro (todos los modelos), iPad Air de tercera generación en adelante, iPad de quinta generación en adelante y iPad mini de quinta generación en adelante.
- iOS 17.0.1 y iPadOS 17.0.1: iPhone XS en adelante, iPad Pro de segunda generación de 12.9 pulgadas y posteriores, iPad Pro de 10.5 pulgadas, iPad Pro de 11 pulgadas de primera generación en adelante, iPad Air de tercera generación en adelante, iPad de sexta generación en adelante y iPad mini de quinta generación en adelante.
- macOS Monterey 12.7 y macOS Ventura 13.6.
- watchOS 9.6.3 y watchOS 10.0.1: Apple Watch Series 4 en adelante.
- Safari 16.6.1: macOS Big Sur y macOS Monterey.

Se atribuye el descubrimiento y reporte de estas deficiencias a Bill Marczak de Citizen Lab de la Universidad de Toronto y a Maddie Stone del Grupo de Análisis de Amenazas (TAG) de

Google, lo que indica que podrían haber sido utilizadas como parte de ataques altamente dirigidos contra miembros de la sociedad civil en mayor riesgo de amenazas cibernéticas.

Esta divulgación se produce dos semanas después de que Apple resolviera otras dos vulnerabilidades zero-day activamente explotadas (CVE-2023-41061 y CVE-2023-41064) que se habían encadenado como parte de una cadena de exploits de iMessage de cero clic llamada BLASTPASS para implementar un spyware mercenario conocido como Pegasus.

Esto fue seguido por Google y Mozilla, que emitieron correcciones para contener una vulnerabilidad de seguridad (CVE-2023-4863) que podría dar como resultado la ejecución de código arbitrario al procesar una imagen especialmente diseñada.

Hay evidencia que sugiere que tanto CVE-2023-41064, una vulnerabilidad de desbordamiento de búfer en el marco de análisis de imágenes Image I/O de Apple, como CVE-2023-4863, un desbordamiento de búfer de montón en la biblioteca de imágenes WebP (libwebp), podrían referirse al mismo error, según Ben Hawkes, fundador de Isosceles y exinvestigador de Google Project Zero.

Rezilion, en un análisis publicado el jueves, reveló que la biblioteca libwebp se utiliza en varios sistemas operativos, paquetes de software, aplicaciones de Linux e imágenes de contenedor, destacando que el alcance de la vulnerabilidad es mucho más amplio de lo que inicialmente se pensaba.

> *«La buena noticia es que el error parece haberse parcheado correctamente en la versión principal de libwebp, y ese parche se está propagando a todos los lugares donde debería llegar. La mala noticia es que libwebp se utiliza en muchos lugares, y podría llevar un tiempo hasta que el parche se implemente completamente»*, dijo Hawkes.