Vulnerabilidades zero-day en iOS y iPadOS de Apple

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Apple ha publicado avisos de seguridad, donde se tratan **2 vulnerabilidades** zero-day que afectan al **Kernel de iOS y iPadOS**, y al componente **RTKit**. Los identificadores de estas vulnerabilidades son CVE-2024-23225 y CVE-2024-23296 y conducen a una condición de corrupción de la memoria.

Desde Apple se afirma tener conocimiento de informes que indican que estos problemas pueden haber sido **explotados activamente.**

Las vulnerabilidades de momento no tienen asignada una puntuación de acuerdo con la escala CVSSv3, pero han sido calificadas por el fabricante como de tipo zero-day, por lo tanto, se le asigna una **severidad crítica**.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

- iOS 17.4 y iPadOS 17.4 con impacto en los productos:

  iPhone XS y posteriores, iPad Pro de 12.9 pulgadas 2da generación y posteriores, iPad Pro de 10.5 pulgadas, iPad Pro de 11 pulgadas 1ra generación y posteriores, iPad Air 3ra generación y posteriores, iPad de 6ta generación y posteriores, y iPad mini 5ta generación y posteriores.

- iOS 16.7.6 y iPadOS 16.7.6 con impacto en los productos:

  iPhone 8, iPhone 8 Plus, iPhone X, iPad de 5ta generación, iPad Pro de 9.7 pulgadas y iPad Pro de 12.9 pulgadas 1ra generación.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso, **que pueden haber sido explotadas**, son los siguientes:

CVE-2024-23225: vulnerabilidad de corrupción de memoria donde un atacante con, capacidad arbitraria de lectura y escritura del kernel, puede eludir las protecciones de la memoria de este.

CVE-2024-23296: vulnerabilidad de corrupción de la memoria donde un atacante, con capacidad arbitraria de lectura y escritura del kernel, puede eludir las protecciones de la memoria de este.

4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Es importante que se tomen medidas rápidamente para solucionar los errores destacados. Por ello, dada la gravedad de las vulnerabilidades, se recomienda aplicar la actualización proporcionada por la compañía actualizando los sistemas operativos iOS y iPadOS.

Las actualizaciones mencionadas pueden encontrarse a través del siguiente enlace:

- https://developer.apple.com/news/releases/

Para facilitar la instalación, se recomienda seguir las instrucciones ofrecidas por el fabricante, que se adjuntan a continuación:

- https://support.apple.com/es-es/HT204204

Debido a que se trata de **vulnerabilidades** de tipo **zero-day**, el equipo de Apple recomienda encarecidamente a los usuarios que lleven a cabo lo antes posibles la actualización correspondiente de dichos productos.

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-23225.
- CVE-2024-23296.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY