Basque CyberSecurity Centre

Actualización de seguridad de Apple-Febrero 2023

BCSC-ACTUALIZACIONES-APPLE-2023-FEBRERO

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Resumen ejecutivo 4
2. Recursos afectados 5
3. Análisis técnico 6
4. Mitigación / Solución 8
5. Referencias Adicionales 9

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.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

A lo largo del mes de febrero Apple ha publicado 5 actualizaciones de seguridad, con vulnerabilidades asociadas, en donde se corrigen 4 fallos que afectan al navegador Safari y a los sistemas operativos iOS, macOS Ventura, watchOS, iPadOS y tvOS.

Los tipos de vulnerabilidades tratadas corrigen fallos de:

- Ejecución de código arbitrario.
- Ejecución de código arbitrario con privilegios de Kernel.
- Denegación de servicio.
- Problema de acceso a datos de usuario desprotegidos.

Dentro de ellas destaca la vulnerabilidad zero-day, cuyo identificador es CVE-2023-23529, y de la que Apple afirma tener el conocimiento de estar siendo **explotada activamente** en la red.

2. Recursos afectados

Las actualizaciones de seguridad del mes de febrero de 2023 están asociadas a vulnerabilidades que afectan a los siguientes productos:

Actualización	Sistemas Afectados	Fecha
macOS Big Sur 11.7.4 Esta actualización no tiene entradas CVE publicadas.	macOS Big Sur	15 de febrero de 2023
Safari 16.3	macOS Big Sur y macOS Monterey	13 de febrero de 2023
iOS 16.3.1 y iPadOS 16.3.1	• iPhone 8 y versiones posteriores • Todos los modelos de iPad • iPad Air de 3º generación y posteriores • iPad de 5º generación y posteriores • iPad mini de 5º generación y posteriores	13 de febrero de 2023
macOS Ventura 13.2.1	macOS Ventura	13 de febrero de 2023
tvOS 16.3.2	Todos los modelos de Apple TV 4K y Apple TV HD	13 de febrero de 2023
watchOS 9.3.1	Apple Watch Series 4 y versiones posteriores	13 de febrero de 2023
tvOS 16.3.1 Esta actualización no tiene entradas CVE publicadas.	Todos los modelos de Apple TV 4K y Apple TV HD	6 de febrero de 2023

3. Análisis técnico

Las vulnerabilidades más relevantes corregidas con esta actualización son:

CVE-2023-23529: vulnerabilidad de confusión de tipos solucionada en macOS Ventura 13.2.1, iOS 16.3.1, iPadOS 16.3.1 y Safari 16.3, de forma que, el procesamiento de contenido web creado con fines malintencionados puede dar lugar a la ejecución de código arbitrario. Apple está al tanto de un informe de que este problema puede haber sido **explotado activamente**.

CVE-2023-23514: vulnerabilidad Use-After-Free solucionada mejorando la administración de la memoria en macOS Ventura 13.2.1, iOS 16.3.1 y iPadOS 16.3.1. Una aplicación puede ejecutar código arbitrario con privilegios de Kernel.

CVE-2023-23524: vulnerabilidad de denegación de servicio solventada corrigiendo la validación de entrada. Este problema se solucionó en macOS Ventura 13.2.1, iOS 16.3.1 y iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. El procesamiento de un certificado creado con fines malintencionados puede provocar una denegación de servicio.

CVE-2023-23522: vulnerabilidad que produce un problema de privacidad corregido mejorando el manejo de los archivos temporales. Este fallo se solucionó en macOS Ventura 13.2.1. Una aplicación puede ser capaz de observar datos de usuario desprotegidos.

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

CVE	Título	Herramientas afectadas	Información adicional
CVE-2023-23529	Contenido de seguridad para Safari 16.3	-WebKit	https://support.apple.com/es-es/HT213638
CVE-2023-23514 CVE-2023-23524 CVE-2023-23529	Contenido de seguridad para iOS 16.3.1 y iPadOS 16.3.1	-Kernel -Security -WebKit	https://support.apple.com/es-es/HT213635

CVE-2023-23514 CVE-2023-23524 CVE-2023-23522 CVE-2023-23529	Contenido de seguridad para macOS Ventura 13.2.1	-Kernel -Security -Shortcuts -WebKit	https://support.apple.com/es-es/HT213633
CVE-2023-23524	Contenido de seguridad para tvOS 16.3.2	-Security	https://support.apple.com/es-es/HT213632
CVE-2023-23524	Contenido de seguridad para watchOS 9.3.1	-Security	https://support.apple.com/es-es/HT213634

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades Apple publica las actualizaciones de seguridad pertinentes, que se encuentran disponibles en Apple Security Updates.

5. Referencias Adicionales

- https://support.apple.com/es-es/HT213638
- https://support.apple.com/es-es/HT213635
- https://support.apple.com/es-es/HT213633
- https://support.apple.com/es-es/HT213632
- https://support.apple.com/es-es/HT213634

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA