Basque CyberSecurity Centre

Actualización de seguridad de Apple-Octubre 2022

BCSC-ACTUALIZACIONES-APPLE-2022-OCTUBRE

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

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.

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

Apple ha publicado 133 actualizaciones de seguridad durante el mes de octubre de 2022, que afectan al navegador Safari, al sistema operativo macOS en sus versiones Ventura, Monterey y Big Sur, al sistema operativo tvOS para Apple TV, al sistema operativo watchOS para los dispositivos Apple Watch, y al sistema operativo iOS para dispositivos Iphone e IPadOS para dispositivos IPad. Dentro de estas actualizaciones se corrigen vulnerabilidades de ejecución de código arbitrario, de escalada de privilegios, de fuga de información y de denegación de servicio.

Particularmente importantes es el fallo zero-day con el identificador CVE-2022-42827, del que Apple asegura tener conocimiento de estar **siendo explotado**.

2. Recursos afectados

Las actualizaciones de seguridad del mes de octubre de 2022 están asociadas a vulnerabilidades que afectan a los siguientes productos:

Actualización	Sistemas Afectados	Fecha
iOS 15.7.1 and iPadOS 15.7.1	iPhone 6s y versiones posteriores,todos los modelos de iPad Pro, iPad Air 2 y versiones posteriores, iPad 5º generación y versiones posteriores, iPad mini 4 y versiones posteriores, y iPod touch de 7º generación	27 de octubre de 2022
Safari 16.1	macOS Big Sur y macOS Monterey	24 de octubre de 2022
iOS 16.1 y iPadOS 16	iPhone 8 y versiones posteriores, todos los modelos de iPad Pro, iPad Air 3º generación y versiones posteriores, iPad 5º generación y posteriores, iPad mini 5º generación y versiones posteriores	24 de octubre de 2022
macOS Big Sur 11.7.1	macOS Big Sur	24 de octubre de 2022
macOS Monterey 12.6.1	macOS Monterey	24 de octubre de 2022
macOS Ventura 13	Mac Studio 2022, Mac Pro 2019 y versiones posteriores, MacBook Air 2018 y versiones posteriores, MacBook Pro 2017 y versiones posteriores, Mac mini 2018 y versiones posteriores, iMac 2017 y versiones posteriores, MacBook 2017, y iMac Pro 2017	24 de octubre de 2022
tvOS 16.1	Apple TV 4K, Apple TV 4K 2º generación, y Apple TV HD	24 de octubre de 2022
watchOS 9.1	Apple Watch Series 4 y versiones posteriores	24 de octubre de 2022

iOS 16.0.3	Iphone 8 y versiones posteriores	10 de octubre de 2022
watchOS 9.0.2 Esta actualización no tiene entradas CVE publicadas.	Apple Watch Series 4 y versiones posteriores	10 de octubre de 2022

3. Análisis técnico

La vulnerabilidad más relevante corregida con esta actualización es:

CVE-2022-42827: vulnerabilidad de ejecución de código arbitrario con privilegios de Kernel de la que Apple asegura tener conocimiento de estar **siendo explotada** y que expone a los dispositivos iPhone e iPad a ataques de ejecución de código arbitrario con privilegios de Kernel, lo que incrementa su severidad y su impacto. Este fallo se abordó el 24 de octubre para corregirlo en iPhone 8 y versiones posteriores, todos los modelos de iPad Pro, iPad Air 3º generación y versiones posteriores, iPad 5º generación y posteriores, iPad mini 5º generación y versiones posteriores y de nuevo el 27 para aportar su corrección a dispositivos más antiguos (iPhone 6s y versiones posteriores, todos los modelos de iPad Pro, iPad Air 2 y versiones posteriores, iPad 5º generación y versiones posteriores, iPad mini 4 y versiones posteriores, y iPod touch de 7º generación).

En cuanto a la métrica de la vulnerabilidad, no está disponible ya que se encuentra actualmente en análisis y no se dispone de información.

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

CVE	Título	Herramientas afectadas	Información adicional
CVE-2022-32932 CVE-2022-42798 CVE-2022-32929 CVE-2022-32935 CVE-2022-32939 CVE-2022-32949 CVE-2022-32944 CVE-2022-42803 CVE-2022-32926 CVE-2022-42827 CVE-2022-42801 CVE-2022-42810 CVE-2022-32941 CVE-2022-42817 CVE-2022-32923 CVE-2022-32927 CVE-2022-37434 CVE-2022-42800	Contenido de seguridad para iOS 15.7.1 y iPadOS 15.7.1	Apple Neural Engine Audio Backup FaceTime Graphics Driver Image Processing Kernel Model I/O ppp Safari WebKit Wi-Fi zlib	https://support.apple.com/es-es/HT213490
CVE-2022-42799 CVE-2022-42823 CVE-2022-42824 CVE-2022-32922	Contenido de seguridad para Safari 16.1	WebKit WebKit PDF	https://support.apple.com/es-es/HT213495

CVE-2022-42825 CVE-2022-32940 CVE-2022-42813 CVE-2022-32946 CVE-2022-32947 CVE-2022-42820 CVE-2022-42806 CVE-2022-32924 CVE-2022-42808 CVE-2022-42827 CVE-2022-42829 CVE-2022-42830 CVE-2022-42831 CVE-2022-42832 CVE-2022-42811 CVE-2022-32938 CVE-2022-42799 CVE-2022-42823 CVE-2022-42824 CVE-2022-32922	Contenido de seguridad para iOS 16.1 y iPadOS 16	AppleMobileFileIntegrity AVEVideoEncoder CFNetwork Core Bluetooth GPU Drivers IOHIDFamily IOKit Kernel ppp Sandbox Shortcuts WebKit WebKit PDF	https://support.apple.com/es-es/HT213489
CVE-2022-42825 CVE-2022-28739 CVE-2022-32862	Contenido de seguridad para macOS Big Sur 11.7.1	AppleMobileFileIntegrity Ruby Sandbox	https://support.apple.com/es-es/HT213493
CVE-2022-42825 CVE-2022-28739 CVE-2022-32862	Contenido para macOS Monterey 12.6.1	AppleMobileFileIntegrity Ruby Sandbox	https://support.apple.com/es-es/HT213494
CVE-2022-42795 CVE-2022-32858 CVE-2022-32898 CVE-2022-32899 CVE-2022-32827 CVE-2022-42789 CVE-2022-42825 CVE-2022-32902 CVE-2022-32904 CVE-2022-32890 CVE-2022-42796 CVE-2022-32940 CVE-2022-42819 CVE-2022-42813	Contenido de seguridad macOS Ventura 13	Accelerate Framework Apple Neural Engine AppleAVD AppleMobileFileIntegrity ATS Audio AVEVideoEncoder Calendar CFNetwork ColorSync	https://support.apple.com/es-es/HT213488

CVE-2022-26730		Crash Reporter	
CVE-2022-32867		curl	
CVE-2022-32205		Directory Utility	
CVE-2022-32206		DriverKit	
CVE-2022-32207		Exchange	
CVE-2022-32208		Find My	
CVE-2022-42814		Finder	
CVE-2022-32865		GPU Drivers	
CVE-2022-32915		Grapher	
CVE-2022-32928		Heimdal	
CVE-2022-42788		Image	
CVE-2022-32905		Processing	
CVE-2022-32947		ImageIO	
CVE-2022-42809		Intel Graphics	
CVE-2022-3437		Driver	
CVE-2022-32913		IOHIDFamily	
CVE-2022-1622		IOKit	
CVE-2022-32936		Kernel	
CVE-2022-42820		Mail	
CVE-2022-42806		Maps	
CVE-2022-32864		MediaLibrary	
CVE-2022-32866		ncurses	
CVE-2022-32911		Notes	
CVE-2022-32924		Notifications	
CVE-2022-32914		PackageKit	
CVE-2022-42808		Photos	
CVE-2022-42815		ppp	
CVE-2022-32883		Ruby	
CVE-2022-32908		Sandbox	
CVE-2021-39537		Security	
CVE-2022-29458		Shortcuts	
CVE-2022-42818		Sidecar	
CVE-2022-32879		Siri	
CVE-2022-32895		SMB	
CVE-2022-32918		Software Update	
CVE-2022-42829		SQLite	
CVE-2022-42830		Vim	
CVE-2022-42831		Weather	
CVE-2022-42832		WebKit	
CVE-2022-28739		WebKit PDF	
CVE-2022-32881		WebKit	
CVE-2022-32862		Sandboxing	
CVE-2022-42811			
CVE-2022-42793			
CVE-2022-32938			
CVE-2022-42790			
CVE-2022-32870			

CVE-2022-32934 CVE-2022-42791 CVE-2021-36690 CVE-2022-0261 CVE-2022-0318 CVE-2022-0319 CVE-2022-0351 CVE-2022-0359 CVE-2022-0361 CVE-2022-0368 CVE-2022-0392 CVE-2022-0554 CVE-2022-0572 CVE-2022-0629 CVE-2022-0685 CVE-2022-0696 CVE-2022-0714 CVE-2022-0729 CVE-2022-0943 CVE-2022-1381 CVE-2022-1420 CVE-2022-1725 CVE-2022-1616 CVE-2022-1619 CVE-2022-1620 CVE-2022-1621 CVE-2022-1629 CVE-2022-1674 CVE-2022-1733 CVE-2022-1735 CVE-2022-1769 CVE-2022-1927 CVE-2022-1942 CVE-2022-1968 CVE-2022-1851 CVE-2022-1897 CVE-2022-1898 CVE-2022-1720 CVE-2022-2000 CVE-2022-2042 CVE-2022-2124 CVE-2022-2125 CVE-2022-2126 CVE-2022-32875 CVE-2022-32886 CVE-2022-32888 CVE-2022-32912			

CVE-2022-42799 CVE-2022-42823 CVE-2022-42824 CVE-2022-32922 CVE-2022-32892			
CVE-2022-42825 CVE-2022-32940 CVE-2022-42813 CVE-2022-32924 CVE-2022-42808 CVE-2022-42811 CVE-2022-42799 CVE-2022-42823 CVE-2022-42824	Contenido de seguridad para tvOS 16.1	AppleMobileFileIntegrity AVEVideoEncoder CFNetwork Kernel Sandbox WebKit	https://support.apple.com/es-es/HT213492
CVE-2022-42825 CVE-2022-32940 CVE-2022-42813 CVE-2022-32947 CVE-2022-32924 CVE-2022-42808 CVE-2022-42811 CVE-2022-42799 CVE-2022-42823 CVE-2022-42824	Contenido de seguridad para watchOS 9.1	AppleMobileFileIntegrity AVEVideoEncoder CFNetwork GPU Drivers Kernel Sandbox WebKit	https://support.apple.com/es-es/HT213491
CVE-2022-22658	Contenido de seguridad para iOS 16.0.3	Mail	https://support.apple.com/es-es/HT213480

4. Mitigación / Solución

Para la mitigación y el parcheo de todas las vulnerabilidades, Apple publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Apple Security Updates.

5. Referencias Adicionales

- https://support.apple.com/es-es/HT213490
- https://support.apple.com/es-es/HT213495
- https://support.apple.com/es-es/HT213489
- https://support.apple.com/es-es/HT213493
- https://support.apple.com/es-es/HT213494
- https://support.apple.com/es-es/HT213488
- https://support.apple.com/es-es/HT213492
- https://support.apple.com/es-es/HT213491
- https://support.apple.com/es-es/HT213480

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA