Basque CyberSecurity Centre

Actualización de seguridad de Apple-Noviembre 2022

BCSC-ACTUALIZACIONES-APPLE-2022-NOVIEMBRE

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

A lo largo del mes de noviembre Apple ha publicado 6 actualizaciones de seguridad que afectan al sistema operativo iOS para dispositivos Iphone y IPadOS, al sistema operativo macOS en su versión Ventura, al sistema operativo tvOS para Apple TV y a Xcode, el entorno de desarrollo creado por Apple destinado al desarrollo de software para iOS, macOS, watchOS y tvOS.

Estas actualizaciones tienen una severidad asignada que varía entre un carácter alto y moderado y su clasificación según su descripción es la siguiente:

- 3 vulnerabilidades de ejecución arbitraria de código.
- 1 vulnerabilidad de divulgación de información.
- 1 vulnerabilidad de escalada de privilegios.
- 1 vulnerabilidad en la que se solucionan diversos problemas en Git.

2. Recursos afectados

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

Actualización	Sistemas Afectados	Fecha
iOS 16.1.2 Esta actualización no tiene entradas CVE publicadas.	iPhone 8 y versiones posteriores	30 de noviembre de 2022
tvOS 16.1.1 Esta actualización no tiene entradas CVE publicadas.	Apple TV 4K (3ra generación)	16 de noviembre de 2022
iOS 16.1.1 e iPadOS 16.1.1	iPhone 8 y modelos posteriores. Todos los modelos de iPad Pro. iPad Air de 3.ª generación y modelos posteriores. iPad de 5.ª generación y modelos posteriores. iPad mini de 5.ª generación y modelos posteriores.	09 de noviembre de 2022
macOS Ventura 13.0.1	macOS Ventura	09 de noviembre de 2022
Xcode 14.1	macOS Monterey 12.5 y versiones posteriores	01 de noviembre de 2022

3. Análisis técnico

Las vulnerabilidades más relevantes corregidas con esta actualización son:

CVE-2022-39260**:** Git shell es un shell de inicio de sesión restringido que se puede usar para implementar la funcionalidad push/pull de Git a través de SSH. En versiones anteriores a 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3 y 2.37.4, la función que divide los argumentos del comando en una matriz utiliza incorrectamente un entero para representar el número de entradas en la matriz, lo que permite que un actor malicioso desborde intencionalmente el valor de retorno, lo que lleva a escrituras arbitrarias en el heap. Es posible aprovechar este ataque para obtener la ejecución remota de código en una máquina víctima.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-40304: vulnerabilidad en libxml2 en versiones anteriores a la 2.10.3. El fallo se produce en ciertas definiciones de entidades XML no válidas que pueden corromper una clave de tabla hash, lo que podría generar errores lógicos posteriores.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-29187: Las versiones de Git anteriores a 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4 y 2.30.5 son vulnerables a la escalada de privilegios en

todas las plataformas, de manera que, por ejemplo, un usuario podría verse afectado por la vulnerabilidad con identificador CVE-2022-24765, y que al navegar como root en un directorio tmp compartido que sea de su propiedad, se vea afectado por repositorios maliciosos creados dentro por un atacante. Las versiones 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4 y 2.30.5 ya disponen de una actualización para este problema. La forma más sencilla de evitar verse afectado por el exploit descrito es evitar ejecutar Git como root, o un administrador en Windows y, si es necesario, reducir su uso al mínimo. Si bien no es posible una solución alternativa genérica, un sistema podría protegerse del exploit descrito en el ejemplo eliminando cualquier repositorio de este tipo y creando uno como root para bloquear cualquier ataque futuro.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-40303: vulnerabilidad en libxml2, en versiones anteriores a la 2.10.3, de manera que al analizar un documento XML de varios gigabytes con la opción de analizador XML_PARSE_HUGE habilitada, se pueden desbordar varios contadores de enteros, lo que puede producir un fallo de segmentación.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

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

CVE	Título	Herramientas afectadas	Información adicional
CVE-2022-40303 CVE-2022-40304	Contenido de seguridad para iOS 16.1.1 e iPadOS 16.1.1	libxml2	https://support.apple.com/es-es/HT213505
CVE-2022-40303 CVE-2022-40304	Contenido de seguridad para macOS Ventura 13.0.1	libxml2	https://support.apple.com/es-es/HT213504
CVE-2022-29187 CVE-2022-39253 CVE-2022-39260 CVE-2022-42797	Contenido de seguridad para Xcode 14.1	Git IDE Xcode Server	https://support.apple.com/es-es/HT213489

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/HT213505
- https://support.apple.com/es-es/HT213504
- https://support.apple.com/es-es/HT213496

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA