Actualización de seguridad de Apple-Marzo 2024

CYBERZAINTZA- ACTUALIZACIONES-APPLE-2024-MARZO

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 la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca. 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

A lo largo del mes de marzo, **Apple** ha publicado 18 actualizaciones de seguridad en las que se corrigen **83 vulnerabilidades** que afectan a los sistemas operativos iOS, iPadOS, macOS Sonoma, macOS Ventura, macOS Monterey, tvOS, watchOS, visionOS, a la aplicación GarageBand, a XCode y al navegador Safari.

Entre las múltiples vulnerabilidades reportadas, las más graves, de ser explotadas, pueden conducir a condiciones de ejecución de código arbitrario, filtrado de datos de audio, cierre inesperado de aplicaciones, denegación de servicio y elevación de privilegios, entre otros.

Dentro de estas correcciones hay que destacar las **2** nuevas vulnerabilidades zero-day, reportadas por Apple a principios de mes, que **pueden haber sido explotadas activamente** y que afectan al **Kernel de iOS** y **iPadOS**, y al componente **RTKit.**

Para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Recursos afectados

Las actualizaciones de seguridad del mes de marzo de 2024 están asociadas a vulnerabilidades que afectan a los siguientes productos:

Actualización	Sistemas afectados	Fecha
Safari 17.4.1	macOS Monterey macOS Ventura	25 Marzo 2024
macOS Sonoma 14.4.1	macOS Sonoma	25 Marzo 2024
macOS Ventura 13.6.6	macOS Ventura	25 Marzo 2024
iOS 17.4.1 y iPadOS 17.4.1	• iPhone XS y versiones posteriores • iPad Pro-12.9 pulgadas 2º generación y versiones posteriores • iPad Pro-10.5 pulgadas • iPad Pro-11 pulgadas 1º generación y versiones posteriores • iPad Air 3 generación y versiones posteriores • iPad 6 generación y versiones posteriores • iPad mini 5 generación y versiones posteriores	21 Marzo 2024
iOS 16.7.7 y iPadOS 16.7.7	• iPhone 8 • iPhone 8 Plus • iPhone X • iPad 5 generación • iPad Pro-9.7 pulgadas • iPad Pro-12.9 pulgadas 1generación	21 Marzo 2024
visionOS 1.1.1	Apple Vision Pro	21 Marzo 2024
GarageBand 10.4.11	• macOS Ventura • macOS Sonoma	12 Marzo 2024
Safari 17.4	• macOS Monterey • macOS Ventura	07 Marzo 2024
macOS Sonoma 14.4	macOS Sonoma	07 Marzo 2024
macOS Ventura 13.6.5	macOS Ventura	07 Marzo 2024

macOS Monterey 12.7.4	macOS Monterey	07 Marzo 2024
watchOS 10.4	Apple Watch Series 4 y versiones posteriores	07 Marzo 2024
tvOS 17.4	Apple TV HD and Apple TV 4K (todos los modelos)	07 Marzo 2024
visionOS 1.1	Apple Vision Pro	07 Marzo 2024
Xcode 15.3	macOS Sonoma 14 y versiones posteriores	05 Marzo 2024
iOS 17.4 y iPadOS 17.4	• iPhone XS y versiones posteriores • iPad Pro-12.9 pulgadas 2º generación y versiones posteriores • iPad Pro-10.5 pulgadas • iPad Pro-11 pulgadas 1º generación y versiones posteriores • iPad Air 3 generación y versiones posteriores • iPad 6 generación y versiones posteriores • iPad mini 5 generación y versiones posteriores	05 Marzo 2024
iOS 16.7.6 y iPadOS 16.7.6	• iPhone 8 • iPhone 8 Plus • iPhone X • iPad 5 generación • iPad Pro-9.7 pulgadas • iPad Pro-12.9 pulgadas 1º generación	05 Marzo 2024
iOS 15.8.2 y iPadOS 15.8.2	• iPhone 6s (todos los modelos) • iPhone 7 (todos los modelos) • iPhone SE (1º generación) • iPad Air 2 • iPad mini (4º generación), • iPod touch (7º generación)	05 Marzo 2024

3. Análisis técnico

Los detalles de las vulnerabilidades de más relevancia tratadas en este aviso son los siguientes:

CVE-2024-23296: vulnerabilidad de corrupción de memoria con una validación mejorada. Este problema se ha solucionado en iOS 17.4 y iPadOS 17.4. Un atacante con capacidad de lectura y escritura arbitraria en el kernel puede ser capaz de saltarse las protecciones de memoria del kernel. Apple tiene conocimiento de un informe que indica que **este problema puede haber sido explotado**.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 787: Out-of-bounds Write

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: Bajo**
- **Interacción con el usuario: Ninguna**
- **Alcance:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

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. Apple tiene conocimiento de un informe que indica que **este problema puede haber sido explotado**.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 787: Out-of-bounds Write

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: Bajo**
- **Interacción con el usuario: Ninguna**
- **Alcance:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-51385: vulnerabilidad de inyección de comandos OS en ssh en OpenSSH antes de 9.6, que puede ocurrir si un nombre de usuario o nombre de host tiene metacaracteres shell, y este nombre es referenciado por un token de expansión en ciertas situaciones.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.8**

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

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

CVE-2024-23270: vulnerabilidad en donde una aplicación puede ser capaz de ejecutar código arbitrario con privilegios del kernel. Este problema se ha corregido en macOS Monterey 12.7.4, macOS Ventura 13.6.5, macOS Sonoma 14.4, iOS 17.4 y iPadOS 17.4, tvOS 17.4.

La métrica de evaluación de las vulnerabilidades se compone de:

CVSS Base: **7.8**

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-2024-23274: vulnerabilidad de inyección que se ha solucionado en macOS Sonoma 14.4, macOS Monterey 12.7.4 y macOS Ventura 13.6.5. Una aplicación puede ser capaz de elevar privilegios.

La métrica de evaluación de las vulnerabilidades se compone de:

CWE 74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

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: Ninguno**
- **Interacción con el usuario:** Requerida
- **Alcance:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

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

Titulo	Enlace	CVE	Componentes Afectados
Contenido de seguridad para Safari 17.4.1	https://support.apple.com/kb/HT214094	CVE-2024-1580	WebRTC
Contenido de seguridad para macOS Sonoma 14.4.1	https://support.apple.com/kb/HT214096	CVE-2024-1580	CoreMedia, WebRTC
Contenido de seguridad para macOS Ventura 13.6.6	https://support.apple.com/kb/HT214095	CVE-2024-1580	CoreMedia, WebRTC
Contenido de seguridad para iOS 17.4.1 y iPadOS 17.4.1	https://support.apple.com/kb/HT214097	CVE-2024-1580	CoreMedia, WebRTC
Contenido de seguridad para iOS 16.7.7 y iPadOS 16.7.7	https://support.apple.com/kb/HT214098	CVE-2024-1580	CoreMedia, WebRTC
Contenido de seguridad para visionOS 1.1.1	https://support.apple.com/kb/HT214093	CVE-2024-1580	CoreMedia, WebRTC
Contenido de seguridad para GarageBand 10.4.11	https://support.apple.com/kb/HT214090	CVE-2024-23300	GarageBand

Contenido de seguridad para Safari 17.4	https://support.apple.com/kb/HT214089	CVE-2024-23273 CVE-2024-23254 CVE-2024-23263 CVE-2024-23280 CVE-2024-23284	Safari Private Browsing, WebKit, Safari
Contenido de seguridad para macOS Sonoma 14.4	https://support.apple.com/kb/HT214084	CVE-2024-23291 CVE-2024-23276 CVE-2024-23227 CVE-2024-23233 CVE-2024-23269 CVE-2024-23288 CVE-2024-23277 CVE-2024-23247 CVE-2024-23248 CVE-2024-23249 CVE-2024-23250 CVE-2024-23244 CVE-2024-23205 CVE-2022-48554 CVE-2024-23253 CVE-2024-23270 CVE-2024-23257 CVE-2024-23258 CVE-2024-23286 CVE-2024-23234 CVE-2024-23266 CVE-2024-23235 CVE-2024-23265 CVE-2024-23225 CVE-2024-23278 CVE-2024-0258 CVE-2024-23279 CVE-2024-23287 CVE-2024-23264 CVE-2024-23285 CVE-2024-23283 CVE-2023-48795 CVE-2023-51384 CVE-2023-51385 CVE-2022-42816 CVE-2024-23216 CVE-2024-23267 CVE-2024-23268 CVE-2024-23274 CVE-2023-42853 CVE-2024-23275	Accessibility, Admin Framework, Airport, AppleMobileFileIntegrity, Bluetooth, ColorSync, CoreBluetooth - LE, Dock, ExtensionKit, file, Image Capture, Image Processing, ImageIO, Intel Graphics Driver, Kerberos v5 PAM module, Kernel, libxpc, MediaRemote, Messages, Metal, Music, Notes, OpenSSH, PackageKit, Photos, QuartzCore, RTKit, Safari, Safari Private Browsing, Sandbox, Screen Capture, Share Sheet, SharedFileList, Shortcuts, Siri, Spotlight, Storage Services, Synapse, System Settings, TV App, UIKit,

		CVE-2024-23255 CVE-2024-23294 CVE-2024-23296 CVE-2024-23259 CVE-2024-23273 CVE-2024-23238 CVE-2024-23239 CVE-2024-23290 CVE-2024-23232 CVE-2024-23231 CVE-2024-23230 CVE-2024-23245 CVE-2024-23292 CVE-2024-23289 CVE-2024-23293 CVE-2024-23241 CVE-2024-23272 CVE-2024-23242 CVE-2024-23281 CVE-2024-23260 CVE-2024-23246 CVE-2024-23226 CVE-2024-23254 CVE-2024-23263 CVE-2024-23280 CVE-2024-23284	WebKit, AppKit, CoreAnimation, CoreMotion, Endpoint Security, Find My, libarchive, libxml2, Model I/O, Power Management, Storage Driver, SystemMigration, TCC, WebKit
Contenido de seguridad para macOS Ventura 13.6.5	https://support.apple.com/kb/HT214085	CVE-2024-23276 CVE-2024-23227 CVE-2024-23269 CVE-2024-23247 CVE-2024-23218 CVE-2024-23270 CVE-2024-23286 CVE-2024-23257 CVE-2024-23234 CVE-2024-23266 CVE-2024-23265 CVE-2024-23225 CVE-2024-23201 CVE-2024-23278 CVE-2023-28826 CVE-2024-23264 CVE-2024-23283 CVE-2024-23274 CVE-2024-23268 CVE-2024-23275	Admin Framework, Airport, AppleMobileFileIntegrity, ColorSync, CoreCrypto, Image Processing, ImageIO, Intel Graphics Driver, Kerberos v5 PAM module, Kernel, libxpc, MediaRemote, Metal, Notes, PackageKit, Share Sheet, SharedFileList, Shortcuts, Storage Services

		CVE-2024-23267 CVE-2024-23216 CVE-2024-23231 CVE-2024-23230 CVE-2024-23203 CVE-2024-23204 CVE-2024-23245 CVE-2024-23217 CVE-2024-23272	
Contenido de seguridad para macOS Monterey 12.7.4	https://support.apple.com/kb/HT214083	CVE-2024-23276 CVE-2024-23227 CVE-2024-23269 CVE-2024-23247 CVE-2024-23218 CVE-2024-23244 CVE-2024-23270 CVE-2024-23286 CVE-2024-23257 CVE-2024-23234 CVE-2024-23266 CVE-2024-23265 CVE-2024-23225 CVE-2024-23201 CVE-2023-28826 CVE-2024-23264 CVE-2024-23283 CVE-2024-23274 CVE-2024-23268 CVE-2024-23275 CVE-2024-23267 CVE-2024-23216 CVE-2024-23230 CVE-2024-23204 CVE-2024-23245 CVE-2024-23272	Admin Framework, Airport, AppleMobileFileIntegrity, ColorSync, CoreCrypto, Dock, Image Processing, ImageIO, Intel Graphics Driver, Kerberos v5 PAM module, Kernel, libxpc, MediaRemote, Metal, Notes, PackageKit, SharedFileList, Shortcuts, Storage Services
Contenido de seguridad para watchOS 10.4	https://support.apple.com/kb/HT214088	CVE-2024-23291 CVE-2024-23288 CVE-2024-23250 CVE-2022-48554 CVE-2024-23286 CVE-2024-23235 CVE-2024-23265 CVE-2024-23225 CVE-2024-23278 CVE-2024-0258 CVE-2024-23297	Accessibility, AppleMobileFileIntegrity, CoreBluetooth - LE, file, ImageIO, Kernel, libxpc, MediaRemote, Messages, RTKit, Sandbox,

		CVE-2024-23287 CVE-2024-23296 CVE-2024-23239 CVE-2024-23290 CVE-2024-23231 CVE-2024-23289 CVE-2024-23293 CVE-2024-23246 CVE-2024-23226 CVE-2024-23254 CVE-2024-23263 CVE-2024-23280 CVE-2024-23284	Share Sheet, Siri, UIKit, WebKit, CoreAnimation, CoreMotion, Find My, libxml2, Power Management, Software Update, WebKit
Contenido de seguridad para tvOS 17.4	https://support.apple.com/kb/HT214086	CVE-2024-23291 CVE-2024-23288 CVE-2024-23250 CVE-2022-48554 CVE-2024-23270 CVE-2024-23286 CVE-2024-23235 CVE-2024-23265 CVE-2024-23225 CVE-2024-23278 CVE-2024-0258 CVE-2024-23297 CVE-2024-23264 CVE-2024-23296 CVE-2024-23239 CVE-2024-23290 CVE-2024-23293 CVE-2024-23241 CVE-2024-23246 CVE-2024-23226 CVE-2024-23254 CVE-2024-23263 CVE-2024-23280 CVE-2024-23284	Accessibility, AppleMobileFileIntegrity, CoreBluetooth - LE, file, Image Processing, ImageIO, Kernel, libxpc, MediaRemote, Metal, RTKit, Sandbox, Siri, Spotlight, UIKit, WebKit, CoreAnimation, CoreMotion, libxml2, Photos, Power Management, Software Update, WebKit
Contenido de seguridad para visionOS 1.1	https://support.apple.com/kb/HT214087	CVE-2024-23262 CVE-2024-23257 CVE-2024-23258 CVE-2024-23286 CVE-2024-23235 CVE-2024-23265 CVE-2024-23225 CVE-2024-23264 CVE-2024-23295	Accessibility, ImageIO, Kernel, Metal, Persona, RTKit, Safari, UIKit, WebKit, Model I/O,

		CVE-2024-23296 CVE-2024-23220 CVE-2024-23246 CVE-2024-23226 CVE-2024-23254 CVE-2024-23263 CVE-2024-23284	Power Management
Contenido de seguridad para Xcode 15.3	https://support.apple.com/kb/HT214092	CVE-2024-23298	Xcode
Contenido de seguridad para iOS 17.4 y iPadOS 17.4	https://support.apple.com/kb/HT214081	CVE-2024-23243 CVE-2024-23262 CVE-2024-23291 CVE-2024-23288 CVE-2024-23277 CVE-2024-23250 CVE-2024-23205 CVE-2022-48554 CVE-2024-23270 CVE-2024-23286 CVE-2024-23225 CVE-2024-23235 CVE-2024-23265 CVE-2024-23278 CVE-2024-0258 CVE-2024-23297 CVE-2024-23287 CVE-2024-23264 CVE-2024-23240 CVE-2024-23255 CVE-2024-23296 CVE-2024-23220 CVE-2024-23259 CVE-2024-23256 CVE-2024-23273 CVE-2024-23239 CVE-2024-23290 CVE-2024-23231 CVE-2024-23292 CVE-2024-23289 CVE-2024-23293 CVE-2024-23241 CVE-2024-23242 CVE-2024-23246 CVE-2024-23226	Accessibility, AppleMobileFileIntegrity, Bluetooth, CoreBluetooth - LE, ExtensionKit, file, Image Processing, ImageIO, Kernel, libxpc, MediaRemote, Messages, Metal, Photos, RTKit, Safari, Safari Private Browsing, Sandbox, Share Sheet, Shortcuts, Siri, Spotlight, Synapse, UIKit, WebKit, AirDrop, CoreAnimation, CoreMotion, Find My, libxml2, Mail Conversation View, NetworkExtension, Power Management, Settings, Software Update,

		CVE-2024-23254 CVE-2024-23263 CVE-2024-23280 CVE-2024-23284	WebKit
Contenido de seguridad para iOS 16.7.6 y iPadOS 16.7.6	https://support.apple.com/kb/HT214082	CVE-2024-23262 CVE-2024-23218 CVE-2024-23286 CVE-2024-23257 CVE-2024-23225 CVE-2024-23235 CVE-2024-23265 CVE-2024-23278 CVE-2023-28826 CVE-2024-23264 CVE-2024-23283 CVE-2024-23259 CVE-2024-23231 CVE-2024-23204 CVE-2024-23203 CVE-2024-23289 CVE-2024-23246 CVE-2024-23284 CVE-2024-23263	Accessibility, CoreCrypto, ImageIO, Kernel, libxpc, MediaRemote, Metal, Notes, Safari, Share Sheet, Shortcuts, Siri, UIKit, WebKit

4. Mitigación / Solución

Para la mitigación y la actualización de todas las vulnerabilidades Apple publica las actualizaciones de seguridad pertinentes que se encuentran disponibles en Apple Security Updates. Por otra parte, las últimas actualizaciones que ofrece Apple para sus productos pueden consultarse y descargarse desde este enlace.

5. Referencias Adicionales

- https://support.apple.com/en-us/HT201222.
- https://support.apple.com/es-es/HT214094.
- https://support.apple.com/es-es/HT214096.
- https://support.apple.com/es-es/HT214095.
- https://support.apple.com/es-es/HT214097.
- https://support.apple.com/es-es/HT214098.
- https://support.apple.com/es-es/HT214093.
- https://support.apple.com/es-es/HT214090.
- https://support.apple.com/es-es/HT214089.
- https://support.apple.com/es-es/HT214084.
- https://support.apple.com/es-es/HT214085.
- https://support.apple.com/es-es/HT214083.
- https://support.apple.com/es-es/HT214088.
- https://support.apple.com/es-es/HT214086.
- https://support.apple.com/es-es/HT214087.
- https://support.apple.com/es-es/HT214092.
- https://support.apple.com/es-es/HT214081.
- https://support.apple.com/es-es/HT214082.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY