USTIC-AV 11/22. Apple lanza actualizaciones para sus productos que corrigen vulnerabilidades explotadas activamente (15/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, del Centro Criptológico Nacional, avisa de la publicación de **actualizaciones de seguridad para productos Apple que abordan múltiples vulnerabilidades**, **incluyendo una de "día cero" (*zero-day*).**

Detalle

Apple ha lanzado una serie de actualizaciones de seguridad para corregir, entre otras, **una vulnerabilidad de "día cero"** (zero-day), calificada como **crítica** por la compañía y con código **CVE-2022-32917**, que **afecta a sus productos con sistemas operativos iOS, iPadOS, macOS Big Sur y macOS Monterey.**

Se trata de un fallo en el *kernel* que **permite la ejecución de código arbitrario** en los dispositivos vulnerables y puede producir una **corrupción de la memoria**. El resultado de una correcta explotación de dicho error permite a una aplicación local **escalar privilegios** en el sistema.

De acuerdo con la información publicada, **esta vulnerabilidad podría estar siendo explotada activamente por atacantes remotos**, lo que se traduce en un escenario de riesgo para gran parte de los usuarios de los mencionados dispositivos, recomendándose que se apliquen las actualizaciones liberadas.

Además, estos parches de seguridad corrigen otras siete vulnerabilidades, algunas explotadas activamente:

- **CVE-2022-22587 (IOMobileFrameBuffer):** una aplicación maliciosa puede ejecutar código arbitrario con privilegios de *kernel.*
- **CVE-2022-22594 (Almacenamiento WebKit):** un sitio web puede rastrear información confidencial del usuario (conocida públicamente pero no explotada activamente)
- **CVE-2022-22620 (WebKit):** el procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
- **CVE-2022-22674 (controlador de gráficos Intel):** una aplicación puede leer la memoria del *kernel*
- **CVE-2022-22675 (AppleAVD):** una aplicación puede ejecutar código arbitrario con privilegios de *kernel.*
- **CVE-2022-32893 (WebKit):** el procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
- **CVE-2022-32894 (Kernel):** una aplicación puede ejecutar código arbitrario con privilegios de *kernel*

Debido a la criticidad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a las vulnerabilidades.

Versiones y Productos Afectados

- **Versiones:**
    - iOS Versiones 15.0 19A346 - 15.6.1 19G82
    - iPadOS Versiones 19A346 - 15.6.1 19G82
    - macOS Big Sur Versiones 11.0 20A2411 - 11.6.8 20G730
    - macOS Monterey Versiones 12.0 21A344 - 12.5.1 21G83

Productos:

- iPhone 6s y posteriores
- Todos los modelos de IPad Pro
- iPad Air 2 y posteriores
- iPad de 5ª generación y posteriores
- iPad mini 4 y posteriores
- iPod Touch de 7ª generación
- Todos los MAC compatibles con Big Sur y Monterey

Recomendaciones Actualizadas (15/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

Será necesario **implementar los parches de seguridad liberados por el fabricante** lo antes posible, lo que **supondrá actualizar los sistemas operativos a las siguientes versiones**:

- Safari a la versión 16,
- macOS Big Sur a la versión 11.7,
- macOS Monterey a la versión 12.6,
- iOS a la versión 16,
- iPadOS a la versión 15.7.

Las actualizaciones pueden encontrarse en el siguiente enlace:

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

Además, el fabricante proporciona las instrucciones que se adjuntan a continuación con la finalidad de facilitar la correcta aplicación de los parches correspondientes:

- https://support.apple.com/es-es/HT204204
- https://support.apple.com/es-es/HT201541

Referencias

- **Publicaciones sobre las vulnerabilidades y parches de seguridad:**
  - https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/12036-actualizacion-de-seguridad-en-apple.html
  - https://www.incibe.es/protege-tu-empresa/avisos-seguridad/apple-corrige-vulnerabilidades-sus-sistemas-actualiza-1
  - About the security content of iOS 15.7 and iPadOS 15.7.
  - About the security content of macOS Big Sur 11.7.
  - About the security content of macOS Monterey 12.6.
  - Apple fixes eight zero-day used to hack Iphones and Macs this year.
- **Web de parches:**
  - https://developer.apple.com/news/releases/
- **Instrucciones del fabricante:**
  - https://support.apple.com/es-es/HT204204
  - https://support.apple.com/es-es/HT201541

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Apple0922]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud