BOLETÍN DE ALERTA

Boletín Nro.: 2021-25

Fecha de publicación: 24/09/2021

Tema: Vulnerabilidad crítica en productos de Apple.

.

Productos afectados:

- iPhone / iPad (versiones de iOS / iPadOS anteriores a la 14.8).
- Mac (versiones anteriores a macOS Big Sur 11.6).
- Apple watch (versiones anteriores a watchOS 7.6.2).
- Navegador Web Safari (versiones anteriores a 14.1.2)

Descripción:

Apple ha lanzado actualizaciones que corrigen dos fallas críticas de seguridad, identificadas como CVE-2021-30858 y CVE-2021-30860. Según la compañía, ambas vulnerabilidades son de día cero y pueden haber sido explotadas activamente.

- CVE-2021-30858: de severidad alta con una puntuación de 8.8, es una vulnerabilidad Use After Free (UAF) que se debe a un manejo inadecuado de la memoria en el WebKit. Debido a la vulnerabilidad, un actor malintencionado puede realizar ataques de ejecución de código arbitrario en productos vulnerables.

- CVE-2021-30860 (FORCEDENTRY): de severidad alta con una puntuación 7.8, es una vulnerabilidad de desbordamiento de enteros que existe en la biblioteca de representación de imágenes de Apple (CoreGraphics). Debido a la vulnerabilidad, un actor malintencionado puede ejecutar código arbitrario en los productos vulnerables a través de un PDF creado con fines malintencionados. Se trata de una vulnerabilidad del tipo 0-click, es decir, no es necesario que el usuario llegue a abrir el archivo; con solo recibirlo, puede ser explotada. Esta vulnerabilidad no afecta al navegador web Safari.

Cabe mencionar que el exploit de esta vulnerabilidad fue descubierto en el teléfono de un activista saudí infectado con el software espía Pegasus de NSO Group, cuando todavía no se conocía la vulnerabilidad.

Impacto:

La explotación exitosa de las vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario y obtener el control total del sistema.

Solución:

Actualizar los productos afectados a la última versión disponible.

- iOS 14.8 y iPadOS 14.8
- macOS Big Sur 11.6
- watchOS 7.6.2
- Safari 14.1.2

Información adicional:

- https://cybersophia.net/vulnerability/emergency-updates-for-macos-ios-and-safari-cve-2021-30858-cve-2021-30860/
- https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/