Apple lanzó actualizaciones de seguridad para abordar múltiples vulnerabilidades en iOS y macOS, incluyendo una vulnerabilidad de día cero que se ha utilizado en ataques en la naturaleza.

El problema, rastreado como CVE-2022-32917, tiene sus raíces en el componente Kernel y podría permitir que una aplicación maliciosa ejecute código arbitrario con privilegios de kernel.

> *«Apple está al tanto de un informe de que este problema pudo haber sido explotado activamente»*, dijo Apple en una breve declaración.

A un investigador anónimo se le atribuye el informe de la vulnerabilidad. Cabe mencionar que CVE-2022-32917 también es la segunda vulnerabilidad de día cero relacionada con Kernel que Apple remedió en menos de un mes.

Los parches están disponibles en las versiones iOS 15.7, iPadOS 15.7, iOS 16, macOS Big Sur 11.7 y macOS Monterey 12.6. Las actualizaciones de iOS y iPadOS cubren iPhone 6s y posteriores, iPad Pro (todos los modelos), iPad Air 2 y posteriores, iPad de 5° generación y posteriores, iPad mini 4 y posteriores y iPod Touch 7° generación.

Con las últimas correcciones, Apple abordó siete fallas de día cero explotadas activamente y una vulnerabilidad de día cero conocida públicamente desde inicios de año:

- 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

Además de CVE-2022-32917, Apple cubrió 10 agujeros de seguridad en iOS 16, que abarcan Contactos, Kernel Maps, MediaLibrary, Safari y WebKit. La actualización de iOS 16 también se destaca por incorporar un nuevo modo de bloqueo que está diseñado para dificultar los ataques sin clic.

iOS representa además una función llamada Respuesta de seguridad rápida, que hace posible que los usuarios instalen de forma automática correcciones de seguridad en dispositivos iOS sin una actualización completa del sistema operativo.

> *«Las respuestas rápidas de seguridad brindan importantes mejoras de seguridad rápidamente, antes de que se conviertan en parte de otras mejoras en una futura actualización de software»,* dijo Apple en un documento de soporte.

Finalmente, iOS 16 también brinda soporte para claves de acceso en el navegador web Safari, un mecanismo de inicio de sesión sin contraseña que permite a los usuarios iniciar sesión en sitios web y servicios mediante la autenticación a través de Touch ID o Face ID.