Apple lanza actualizaciones urgentes para corregir 0-Day en iPhone y iPad

Autor: I. Stepanenko

Fecha: Sunday 24th of October 2021 05:36:12 AM

Apple lanzó este lunes una actualización de seguridad para iOS y iPad con el fin de abordar una vulnerabilidad crítica que al parecer, está siendo explotada en la naturaleza, lo que la convierte en la vulnerabilidad de día cero número 17 que la compañía ha abordado en sus productos desde inicio del año.

La vulnerabilidad rastreada como CVE-2021-30883, se refiere a un problema de corrupción de memoria en el componente *«IOMobileFrameBuffer»*, que podría permitir que una aplicación ejecute código arbitrario con privilegios del kernel. Al acreditar a un investigador anónimo por informar sobre la vulnerabilidad, Apple dijo que *«está al tanto de un informe de que este problema puede haber sido explotado activamente».*

Los detalles técnicos sobre la falla y la naturaleza de los ataques aún no están disponibles, al igual que la identidad del actor de la naturaleza, para permitir que la mayoría de los usuarios apliquen el parche y evitar que otros adversarios utilicen la vulnerabilidad como arma. Apple

dijo que abordó el problema mejorando el manejo de la memoria.

El investigador de seguridad Saar Amar compartió detalles adicionales y un exploit de prueba de concepto (PoC), y dijo que *«esta superficie de ataque es muy interesante porque es accesible desde la zona de pruebas de la aplicación (por lo que es excelente para los jailbreak) y muchos otros procesos, lo que lo convierte en un buen candidato para exploits de LPE en cadenas».*

CVE-2021-30883 es también el segundo IOMobileFrameBuffer de impacto de día cero después de que Apple abordara un problema similar de corrupción de memoria informado de forma anónima (CVE-2021-30807) en julio de 2021, lo que plantea la posibilidad de que las dos vulnerabilidades puedan estar relacionadas. Con la última solución, la compañía ha resuelto un récord de 17 vulnerabilidades 0-day hasta la fecha solo en 2021:

CVE-2021-1782 (Kernel): Una aplicación malintencionada puede elevar los privilegios
CVE-2021-1870 (Webkit): Un atacante remoto puede provocar la ejecución de código arbitrario
CVE-2021-1871 (Webkit): Un atacante remoto puede provocar la ejecución de código arbitrario
CVE-2021-1879 (Webkit): El procesamiento de contenido web creado con fines malintencionados puede generar secuencias de comandos universales entre sitios
CVE-2021-30657 (Preferencias del sistema): Una aplicación malintencionada puede eludir las comprobaciones de Gatekeeper
CVE-2021-30661 (Webkit Storage): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30663 (Webkit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30665 (Webkit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30666 (Webkit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30713 (marco TCC): Una aplicación malintencionada puede ludir las preferencias

de privacidad
CVE-2021-30761 (Webkit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30762 (Webkit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30807 (IOMobileFrameBuffer): Una aplicación puede ejecutar código arbitrario con privilegios del kernel
CVE-2021-30858 (webkit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30860 (CoreGraphics): El procesamiento de un PDF creado con fines malintencionados puede provocar la ejecución de código arbitrario
CVE-2021-30869 (XNU): Una aplicación maliciosa puede ejecutar código arbitrario con privilegios del kernel
Se recomienda a los usuarios de Apple que actualicen a la última versión (iOS 15.0.2 y iPad 15.0.2) para mitigar la vulnerabilidad.