Apple lanzó este jueves varias actualizaciones de seguridad para parchear tres vulnerabilidades de día cero que se revelaron como explotadas activamente en la naturaleza.

Implementadas como parte de sus actualizaciones para iOS, iPadOS, macOS y watchOS, las vulnerabilidades residen en el componente FontParser y el kernel, lo que permite a los atacantes ejecutar remotamente código arbitrario y ejecutar programas maliciosos con privilegios de nivel de kernel.

Las vulnerabilidades de día cero fueron descubiertas e informadas a Apple por el equipo de seguridad ProjectZero de Google.

«Apple está al tanto de los informes sobre una vulnerabilidad para este problema», dijo Apple sin mencionar detalles adicionales para dar tiempo a los usuarios de instalar las actualizaciones.

La lista de dispositivos afectados incluye iPhone 5s y posteriores, iPod touch de sexta y séptima generación, iPad Air, iPad mini 2 y posteriores y Apple Watch Series 1 y posteriores.

Las correcciones están disponibles en las versiones iOS 12.4.9 y 14.2, iPadOS 14.2, watchOS 5.3.9, 6.2.9 y 7.1, y como actualización complementaria para macOS Catalina 10.15.7.

El boletín de seguridad de Apple menciona las vulnerabilidades:

- CVE-2020-27930: Un problema de corrupción de memoria en la biblioteca FontParser, que permite la ejecución remota de código al procesar una fuente creada con fines malintencionados.
- CVE-2020-27932: Un problema de inicialización de la memoria que permite que una aplicación maliciosa ejecute código arbitrario con privilegios de kernel.
- CVE-2020-27950: Un problema de confusión de tipos que hace posible que una aplicación maliciosa revele la memoria del kernel.

> *«Explotación dirigida en la naturaleza similar a otros 0-day reportados recientemente. No relacionado con ningún objetivo electoral»,* dijo Shane Huntley, director del Grupo de Análisis de Amenazas de Google.

Esta es la divulgación más reciente de vulnerabilidades de día cero que ProjectZero ha informado desde el 20 de octubre. Primero se informó sobre un 0-day en la biblioteca de representación de fuentes FreeType (CVE-2020-15999), después un día cero de Windows (CVE-2020-17087), seguidos de dos más en Chrome y su variante Android (CVE-2020-16009 y CVE-2020-16010).

Se espera que se lance un parche para el día cero de Windows el 10 de noviembre como parte del martes de parches de este mes.