Ian Beer, el hacker de sombrero blanco de Google Project Zero, reveló este martes los detalles de un error crítico «wormable» de iOS, ahora parcheado, que podría haber hecho posible que un atacante remoto obtuviera el control completo de cualquier dispositivo cercano a través de Wi-Fi.

El exploit permite *«ver todas las fotos, leer todo el correo electrónico, copiar todos los mensajes privados y monitorear todo lo que sucede en el dispositivo en tiempo real»*, dijo Beer en una publicación de blog sobre su investigación de seis meses.

La vulnerabilidad, rastreada como CVE-2020-3843, fue abordada por Apple en una serie de actualizaciones de seguridad impulsadas como parte de iOS 13.3.1, macOS Catalina 10.15.3 y watchOS 5.3.7 a inicios de este año.

> *«Un atacante remoto puede causar la terminación inesperada del sistema o dañar la memoria del kernel. El problema de corrupción de la memoria se solucionó con una validación de entrada mejorada»*, dijo Apple.

La vulnerabilidad se debe a un *«error de programación de desbordamiento de búfer bastante trivial»* en un controlador de WiFi asociado con Apple Wireless Direct Link (AWDL), un protocolo de red de malla patentado desarrollado por Apple para su uso en AirDrop, AirPlay, entre otros, que permite comunicaciones más sencillas entre los dispositivos Apple.

En otras palabras, el exploit zero-click utiliza una configuración que consta de un iPhone 11 Pro, Raspberry Pi y dos adaptadores WiFi diferentes para lograr la lectura y escritura arbitrarias de la memoria del kernel remotamente, aprovechándola para inyectar cargas útiles de shellcode en la memoria del kernel a través de un proceso víctima y escapar de las protecciones de la zona de pruebas del proceso para obtener datos del usuario.

El atacante entonces, apunta al marco AirDrop BTLE para habilitar la interfaz AWDL forzando el valor hash de un contacto de una lista de 100 contactos generados de forma aleatoria almacenados en el teléfono, luego explota el desbordamiento del búfer AWDL para obtener

acceso al dispositivo y ejecutar un implante como raíz, lo que le da a la parte maliciosa un control total sobre los datos personales del usuario, incluidos correos electrónicos, fotos, mensajes, datos de iCloud y más.

Aunque no existe evidencia de que la vulnerabilidad haya sido explotada en la naturaleza, el investigador dijo que *«los proveedores de exploits parecían darse cuenta de estas correcciones».*

Esta no es la primera vez que se descubren fallas de seguridad en el protocolo AWDL de Apple. En julio pasado, los investigadores de la Universidad Técnica de Darmstadt, Alemania, revelaron vulnerabilidades en AWDL que permitían a los atacantes rastrear usuarios, bloquear dispositivos e incluso interceptar archivos transferidos entre dispositivos a través de ataques man-in-the-middle (MitM).

Synacktiv detalla la vulnerabilidad de día cero «Memory Leak» parcheada por Apple

Además, en un desarrollo separado, Synacktiv compartió más detalles sobre CVE-2020-27959, una de las tres vulnerabilidades explotadas activamente que Apple corrigió el mes pasado luego de un informe de Google Project Zero.

Aunque las divulgaciones fueron escasas en detalles, las vulnerabilidades fueron el resultado de un problema de corrupción de memoria en la biblioteca FontParser, que permitió la ejecución remota de código, una fuga de memoria que otorgó al kernel de una aplicación maliciosa privilegios para ejecutar código arbitrario y una confusión de tipos en el núcleo.

Al comparar los dos binarios del kernel asociados con iOS 12.4.8 y 12.4.9, los investigadores de Synacktiv pudieron rastrear las raíces del problema de fuga de memoria, señalando explícitamente que los cambios abordan cómo el kernel maneja los mensajes mach asociados con la comunicación entre procesos en dispositivos Apple.

Los investigadores también idearon un código de prueba de concepto que explota la falla para filtrar de forma confiable una dirección de kernel de puerto mach.

> *«Es bastante sorprendente cuánto tiempo ha sobrevivido esta vulnerabilidad en XNU sabiendo que el código es open source y que cientos de hackers han auditado en gran medida»,* dijo *Fabien Perigaud*, de Synacktiv.