Investigadores de seguridad cibernética de Google finalmente revelaron detalles y exploits de prueba de concepto para 4 de 5 vulnerabilidades que podrían permitir a los hackers remotos apuntar a dispositivos Apple simplemente enviando un mensaje creado maliciosamente por medio de iMessage.

Las vulnerabilidad, que no requieren interacción del usuario, fueron reportadas de forma responsable a Apple por Samuel Grob y Natalie Silvanovich, de Google Project Zero, dichas vulnerabilidades fueron parcheadas la semana pasada con la actualización 12.4 de iOS.

Cuatro de las vulnerabilidades son problemas de *«interacción sin uso»* que causan daños en la memoria que podrían permitir a los atacantes remotos lograr la ejecución de código arbitrario en los dispositivos iOS afectados.

Sin embargo, los investigadores publicaron detalles y exploits para tres de las cuatro vulnerabilidades críticas de RCE y mantuvieron una privada (CVE-2019-8641) porque la última actualización del parche no abordó por completo este problema.

La quinta vulnerabilidad (CVE-2019-8646), una lectura fuera de límites, también se puede ejecutar de remotamente al enviar un mensaje con formato incorrecto a través de iMessage. Pero en lugar de ejecución del código, el error permite al atacante leer el contenido de los archivos almacenados en el dispositivo iOS de la víctima a través de la memoria filtrada.

Los detalles breves, enlaces al aviso de seguridad y vulnerabilidades de PoC para las cuatro vulnerabilidades se listan a continuación:

- CVE-2019-8647 (RCE a través de iMessage): Es una vulnerabilidad sin uso que reside en el marco de Core Data de iOS, que puede causar la ejecución de código arbitrario debido a la deserialización insegura cuando se utiliza el método NSArray initWithCoder.
- CVE-2019-8662 (RCE a través de iMessage): Esta vulnerabilidad es similar a la anterior, de uso libre y reside en el componente QuickLock de iOS, que también se puede activar de forma remota por medio de iMessage.

- CVE-2019-8660 (RCE a través de iMessage): Es un problema de corrupción de memoria que reside en el marco Core Data y el componente Siri, que de ser explotado exitosamente, podría permitir a los atacantes remotos causar la finalización inesperada de la aplicación o la ejecución de código arbitrario.
- CVE-2019-8646 (Lectura de archivos a través de iMessage): Esta falla también residen en los componentes Siri y Core Data, y podría permitir a un hacker leer el contenido de los archivos almacenados en dispositivos iOS de forma remota sin interacciones del usuario, como usuario móvil con no-sandbox.

Además de estas cinco vulnerabilidades, Silvanovich también publicó la semana pasada detalles y una vulnerabilidad de PoC para otra vulnerabilidad de lectura fuera de límites que permite a los atacantes remotos perder memoria y leer archivos desde un dispositivo remoto.

La vulnerabilidad, asignada como CVE-2019-8624, reside en el componente Digital Touch de WatchOS, y afecta a Apple Watch Series 1 y posterior. Apple solucionó este problema en este mes con el lanzamiento de WatchOS 5.3.

Ya que las vulnerabilidades de prueba de concepto para esta seis vulnerabilidades de seguridad ahora están disponibles para el público, se recomienda a los usuarios que actualicen sus dispositivos Apple a la última versión del software lo antes posible.

Además de las vulnerabilidades de seguridad, las tan esperadas actualizaciones de iOS 12.4 para iPhone, iPad y iPod touch también presentaron algunas características nuevas, incluida la capacidad de transferir datos de forma inalámbrica y migrar directamente desde un iPhone antiguo a uno nuevo durante la configuración.