CIENCIA Y TECNOLOGÍA

Riesgos de vulnerabilidades: Descubren cómo robar las fotos borradas en un iPhone X

El Ciudadano · 16 de noviembre de 2018

Los expertos demostraron en ujn concurso tecnológico en Tokio cómo se puede 'hackear' un iPhone X con la última versión de iOS 12.1 instalada para obtener estas imágenes eliminadas

Una vez más los expertos en seguridad tecnológica han demostrado en el evento en Tokio de Mobile Pwn2Own, un concurso de 'hackeo' informático, que los dispositivos móviles están en riesgo de vulnerabilidades.

«Nos sorprendió ver cuán popular era el teléfono Xiaomi, con cinco objetivos», dijo a *eWEEK* Dustin Childs, gerente de comunicaciones de ZDI. «Otra sorpresa positiva fue un día lleno de éxitos en el Día 1. Eso es una rareza para Pwn2Own».

En el Mobile Pwn2Own de 2017, ZDI otorgó a los investigadores un total de $ 515,000 por revelar 32 vulnerabilidades.En Mobile Pwn2Own 2018, celebrado en Tokio del 13 al 14 de noviembre, el Zero Day Initiative (ZDI) de Trend Micro otorgó un total de $ 325,000 a los investigadores de seguridad.

Durante el evento de dos días, los investigadores informaron más de 16 nuevas vulnerabilidades, exponiendo riesgos en los teléfonos Apple iPhone, Samsung Galaxy S9 y Xiaomi Mi6 totalmente parcheados.

https://twitter.com/CaraWainwright7/status/1063323755286544384

Vulnerabilidades

Dos expertos en ciberseguridad, Richard Zhu y Amat Kama, encontraron la manera de «robar» fotos eliminadas de un iPhone X. Los expertos, que forman el equipo Fluoroacetate, hicieron en Tokio una demostración de un ataque simulado durante el Mobile Pwn2Own, y recibieron de los organizadores un premio de **50.000 de dólares** por detectar ese error, informa el portal Eweek.

Los usuarios de iPhones saben que al eliminar una foto, el sistema operativo iOS advierte que la imagen se borrará del archivo iCloud Photo en todos los dispositivos. Cuando el usuario confirma esta acción, la foto se mueve a la carpeta 'Eliminado'. Desde ahí se puede restaurar o eliminar la imagen de forma permanente. Si no haces nada, la foto desaparecerá automáticamente al cabo de 30 días.

Los expertos demostraron cómo se puede 'hackear' un iPhone X con la última versión de iOS 12.1 instalada para obtener estas imágenes eliminadas.

Team Fluoroacetate.

Resulta que el llamado compilador JIT (que ejecuta el código del programa durante el trabajo de la aplicación y no antes de su iniciación) contiene en el navegador Safari una vulnerabilidad que permite a los atacantes **acceder de forma remota a la carpeta «Eliminado» y robar imágenes borradas**.

Según Zhu y Kama, el ataque puede llevarse a cabo a través de un punto de acceso Wi-Fi malicioso, por ejemplo, una cafetería o un aeropuerto. Los 'hackers' han notificado a Apple el error, pero hasta ahora no ha sido solucionado.

Los dispositivos Android también son vulnerables. Tras recurrir a una tecnología similar, los especialistas de F-Secure MWR Labs pudieron obtener datos del Samsung Galaxy S9 y Xiaomi Mi6.

El equipo conocido como Fluoroacetate terminó ganando el evento general al demostrar múltiples vulnerabilidades. El primer error demostrado por el equipo de Fluoroacetate fue un problema de NFC (comunicaciones de campo cercano) en el teléfono Xiaomi Mi6. Ese error ganó Fluoroacetate $ 30,000.

«Al usar la función de toque para conectar, forzaron al teléfono a abrir el navegador web y navegar a su página web especialmente diseñada», escribió el blog de Childs. «La página web explotó una escritura Out-of-Bounds en WebAssembly para obtener la ejecución del código en el teléfono».

Fluoroacetate también explotó el Samsung Galaxy S9 a través de una vulnerabilidad en el componente de banda base del teléfono. ZDI otorgó $ 50,000 para la emisión de banda base, lo que permitió un desbordamiento del montón de memoria.

Continúa leyendo...

https://www.elciudadano.cl/ciencia-tecnologia/apple-revela-una-grave-falla-que-presenta-el-costoso-iphone-x/11/13/

https://www.elciudadano.cl/tecnologia-2/confirmado-por-apple-el-iphone-5-entro-en-la-lista-de-equipos-obsoletos/11/02/

Fuente: El Ciudadano