Alerta: una falla en los cargadores rápidos de celulares puede provocar incendios

26/07/2020

Un estudio de investigadores de seguridad de Xuanwu Lab, que operan bajo el gigante tecnológico chino Tencent alertó sobre una vulnerabilidad muy peligrosa en los cargadores rápidos de celulares.

Se trata de una alteración que se puede hacer en el firmware del cargador, para alterar el voltaje y acelerar los procesos de acumulación de batería de los dispositivos conectados, lo que de paso los pone en peligro de derretimiento e incendio.

Esta especie de hackeo permitiría sacar los componentes de seguridad al firmware, los que justamente protegen contra sobrecarga, sobrecalentamiento y otros riesgos de seguridad.

El ataque fue apodado por los investigadores como Badpower, y ellos mismos explican en qué consiste el problema:

“Algunos fabricantes han diseñado interfaces que pueden leer y escribir el firmware incorporado en el canal de datos, pero no han realizado una verificación de seguridad efectiva en el comportamiento de lectura y escritura, o hay un problema en el proceso de verificación, o hay ciertos problemas de corrupción de memoria en la implementación del protocolo de carga rápida. Un atacante podría usar estos problemas para reescribir el firmware del dispositivo de carga rápida para controlar el comportamiento de la fuente de alimentación del dispositivo”, sostienen.

Así, el estudio explica en tres pasos cómo se puede provocar un incendio:

– El atacante invade el teléfono móvil, la computadora portátil y otros dispositivos terminales del usuario de alguna manera, e implanta programas maliciosos con capacidades de ataque BadPower, convirtiendo el dispositivo terminal en un agente de ataque BadPower.

– Cuando el usuario conecta el dispositivo terminal al cargador, un programa malicioso en el dispositivo terminal invade el firmware interno del cargador.

– Cuando el usuario usa el cargador invadido para cargar el dispositivo nuevamente, el cargador realizará un ataque de sobrecarga de energía en el dispositivo alimentado.

El estudio arrojó que hay al menos 234 dispositivos de carga rápida en el mercado. De 35 probados, al menos 18 tenían problemas de BadPower e involucraban 8 marcas. Entre los 18 modelos, 11 pueden ser atacados a través de terminales digitales que admiten carga rápida. Al mismo tiempo, los investigadores chinos, encuestaron a 34 fabricantes de chips de carga rápida y descubrieron que al menos 18 fabricantes de chips producen éstos con la capacidad de actualizar el firmware después de que el producto fue terminado.