Wi-Fi vulnerable: más de mil millones de dispositivos afectados por una falla de seguridad

27/02/2020

Expertos en seguridad informática descubrieron una vulnerabilidad de amplísimo alcance, que afecta a miles de millones de dispositivos en el mundo. Se trata de una falla en chips Wi-Fi de Broadcom y Cypress, componentes que son utilizados en numerosos equipos con Android, iOS, productos de Amazon y Apple, computadoras y routers de diversas marcas.

Los investigadores realizaron pruebas similares en chips de Realtek, Mediatel, Qualcomm y Realink, notando que los mismos no son vulnerables.

Bautizado "**Kr00k**", el fallo permite que un atacante acceda a información que se envía vía Wi-Fi. Tal como comentan en *Technology Review*, los diferentes fabricantes lanzaron parches para remediarlo, aunque teniendo en cuenta la magnitud de la vulnerabilidad es complejo saber cuántos lo han solucionado efectivamente.

Según explicaron desde ESET, la compañía que descubrió la falla, la misma ocurre cuando un dispositivo con un chip de los mencionados fabricantes se desvincula de un punto de acceso Wi-Fi. Es suficiente que uno de los dos dispositivos sea vulnerable (por ejemplo, un teléfono que se vincula a un router) para que "Kr00k" logre su cometido, alterando la clave de la sesión por una compuesta únicamente de ceros.

¿Cuándo ocurre una desvinculación? Constantemente: al apagar el Wi-Fi de un dispositivo, al alejarnos del router al que nos

vinculamos, al pasar a modo avión, etcétera. En esa instancia, un pirata informático puede llevar a cabo su ataque.

Eso sí: la intrusión es de sencilla detección ya que el atacante precisa realizar constantes conexiones y desconexiones para robar un volumen importante de datos.

Entre los confirmados como vulnerables figuran modelos antiguos de iPhone, tablets iPad, equipos Nexus de Google, la minicomputadora Raspberry Pi3, y computadoras MacBook.

Fuente: TN