Fallo de seguridad encontrado en la tecnología Bluetooth pone en peligro la información de millones de dispositivos

Millones de dispositivos en todo el mundo, desde teléfonos hasta computadores, audífonos y equipos de sonido, se vieron afectados por un **fallo crítico en la seguridad de la tecnología que incorpora Bluetooth**.
Los ataques denominados «**Bluffs**» fueron dados a conocer por investigadores de Eurecom, y se trataría de un virus para evadir las medidas de seguridad, poniendo en riesgo la información que sea compartida a través de la red inalámbrica.

Según datos de la investigación, los riesgos de utilizar Bluetooth 4.2 (que está presente en los equipos fabricados desde diciembre de 2014) y hasta Bluetooth 5.4 (puesto en febrero de 2023) son graves.

Esta no es la primera vez que se descubre un error que comprometa la seguridad de millones de usuarios. De hecho, se conoció que entre los dispositivos afectados se encuentran los **iPhone, iPad y Mac** que incorporan la tecnología Bluetooth. Sin embargo, en un artículo publicado por el investigador Daniele Antonioli, se explica que un atacante puede manipular el establecimiento de una sesión de Bluetooth para interferir en cualquier tipo de dispositivo.

> ***«El atacante primero instala una clave de sesión débil, luego dedica algún tiempo a forzarla y la reutiliza para hacerse pasar por una víctima o implementar un ataque de intermediario en sesiones posteriores y descifrar datos de sesiones anteriores», explica el investigador Antonioli.***

Por ahora, el grupo de investigadores lanzó un llamado para que los fabricantes como **Google, Qualcomm, Apple, Lenovo e Intel** trabajen en corregir la problemática.

> ***«Diseñamos una función de derivación de claves de sesión Bluetooth compatible con versiones anteriores que se basa en una derivación de claves nueva, autenticada y mutua. Nuestra función detiene los seis ataques BLUFFS y aborda sus causas fundamentales a nivel de protocolo. Mostramos cómo integrar nuestra contramedida en el estándar Bluetooth con una sobrecarga mínima», se lee en un comunicado emitido por Eurecom.***

Consejos para prevenir posibles filtraciones de datos en Bluetooth

Mientras los fabricantes lanzan el parche de seguridad, lo que **se le aconseja a los usuarios es mantener una serie de configuracione**s para evitar posibles filtraciones de los datos.

Algunas de las recomendaciones son:

- Permanecer con el Bluetooth apagado en establecimientos públicos.
- En caso de tener un equipo de Apple, verificar que el sistema se encuentre con el último parche de seguridad.
- Tener actualizado el sistema operativo del dispositivo.
- Evitar compartir información importante a través de sistemas como AirDrop, Bluetooth o WiFi.

Con información de El Nacional