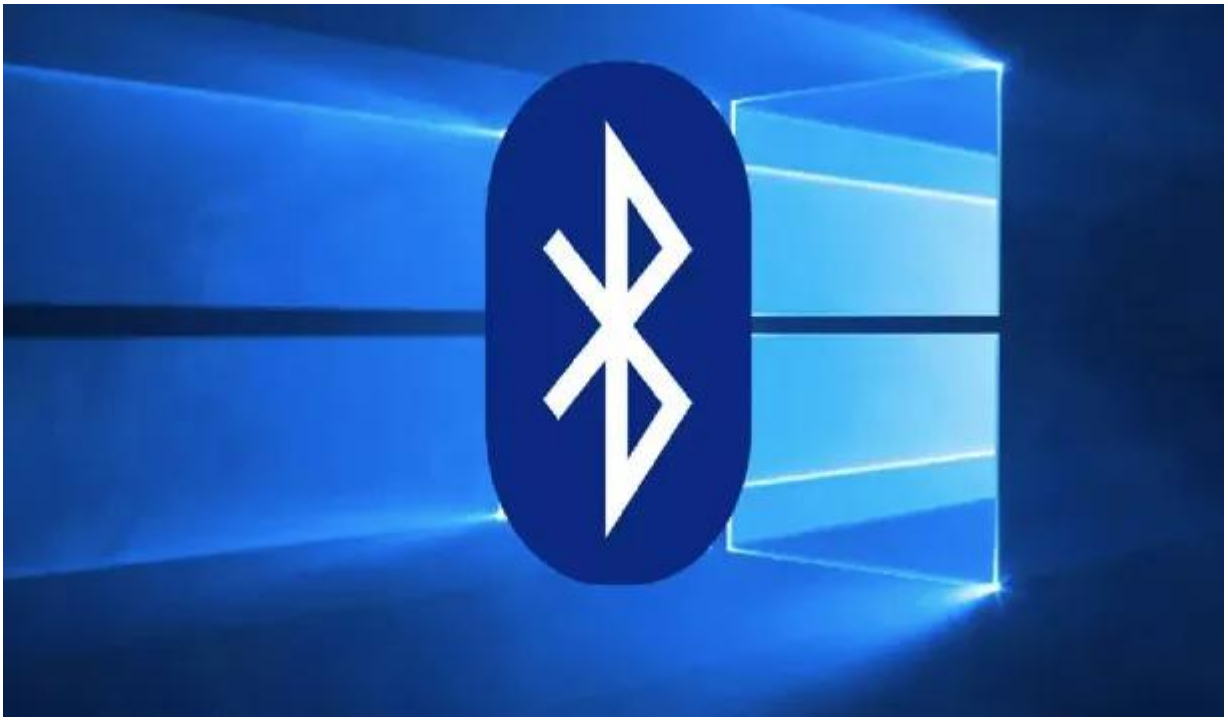
Advierten que el bluetooth pone en peligro la información de los dispositivos

03/07/2022



La tecnología bluetooth, generó a principios de los años 90 una revolución en el ámbito de la comunicación inalámbrica de corto alcance entre dispositivos. Sin embargo, su uso trae aparjado algunos ciberriesgos.

Check Point, un proveedor líder de soluciones de ciberseguridad a nivel mundial, advirtió que el funcionamiento del bluetooth hace que esta tecnología no esté exenta de sufrir vulnerabilidades que permitan a los ciberdelincuentes acceder a los datos de los dispositivos a través de estas conexiones.

Suplantación de bluetooth, robo de datos, bluebugging, bluesnarfing y rastreo de dispositivos, los principales ciberriesgos asociados a la tecnología Blutooth.

Alejandro Botter, gerente de ingeniería de Check Point para el sur de Latinoamérica, dijo: “La tecnología bluetooth nació como solución a los problemas de conectividad por cable. Durante años fue una de las grandes innovaciones y comenzó a utilizarse en teléfonos móviles, ordenadores portátiles, etc., pero con el desarrollo de nuevas tecnologías su uso ha quedado reducido a emparejar dispositivos wearables como relojes inteligentes”.

Según Botter, las conexiones «pueden convertirse en una brecha de seguridad de gran potencial que podría permitir a un ciberdelincuente acceder a una gran cantidad de información de su víctima”, añade Alejandro Botter.

A pesar de que las nuevas versiones de esta tecnología cuentan con cifrado de datos, siguen siendo vulnerables. Se estima que para este 2022 el número total de dispositivos equipados con Bluetooth supere los 5.000 millones. **Check Point Software señaló los principales peligros de esta tecnología:**

Bluebugging

Con este ciberataque se **puede controlar de forma remota varios aspectos de un celular, como realizar llamadas o enviar mensajes, e incluso acceder a un registro de las pulsaciones realizadas.**

El delincuente accede al teléfono a través de la conexión bluetooth para crear una “puerta trasera” (backdoor) en el sistema operativo del terminal y puede controlar por completo el equipo infectado.

Bluesnarfing

Se trata de un tipo de **ataque informático que permite a un ciberdelincuente acceder a datos personales como fotografías, vídeos, eventos en el calendario, etc.**

El atacante se aprovecha de que un dispositivo tenga el

Bluetooth encendido y esté en modo “visible para todo el mundo”, lo cual podría permitir establecer una conexión de emparejamiento sin consentimiento y sin que la víctima se dé cuenta de lo que está ocurriendo. De esta forma, **el dispositivo y la información almacenada en él quedan a merced del atacante. ue**

BIAS (Bluetooth Impersonation Attacks)

Este tipo de ataque permitiría a un ciberdelincuente poder suplantar la identidad de un dispositivo y conectarse con otro para lanzar su ataque.

Al emparejar dos equipos, **se produce un intercambio de claves para establecer ese vínculo, una de las cuáles sirve para que, de cara a interacciones posteriore**s, los dispositivos se reconozcan rápidamente.

Aprovecha este código, que no varía, para suplantar a uno de los equipos y establecer conexión con el otro, y así toma el control del dispositivo al que engañó.

Investigaciones demuestran que esta amenaza podría afectar a millones de dispositivos celulares.

Rastreo de dispositivos

Esta tecnología es que puede utilizarse para localizar la ubicación de un dispositivo.

Durante la pandemia, Check Point Software advirtió en una de sus investigaciones que al**gunas aplicaciones de rastreo, entre las que podría encontrarse las destinadas a controlar los contagios por COVID-19, requieren el uso de Bluetooth de baja energía (BLE) para que funcionen.** Así permiten a los dispositivos emitir rangos de señales que facilitan la identificación del contacto con otros dispositivos.

Un cibercriminal podría rastrear el dispositivo de una persona

correlacionando el dispositivo y sus respectivos paquetes de señales de identificación.

Robo de datos y espionaje

Otro consiste en el robo de información e incluso actividades de espionaje (eavesdropping).

El delincuente busca i**nterceptar una transmisión Bluetooth y explotar fallos de seguridad existentes para después acceder a la información guardada o, incluso, poder escuchar** u**#**