¡Cuidado! Esta nueva vulnerabilidad Bluetooth pone en peligro tu móvil

Cuando hablamos de dispositivos Bluetooth, a todos nos viene a la mente nuestro teléfono móvil. El centro neurálgico de todas las conexiones inalámbricas de nuestro hogar ahora se ve expuesto a un nuevo problema de seguridad detectado por las organizaciones detrás de esta tecnología inalámbrica.

Hace unas horas se han publicado una serie de consejos que todos los fabricantes de dispositivos móviles, así como proveedores, deberías seguir para enfrentarse a un nuevo ataque, denominado BLURtooth, dirigido a los dispositivos con capacidades Bluetooth.

Estos expertos aseguran que se trata de una vulnerabilidad en un componente del estándar Bluetooth denominado Cross-Transport Key Derivation (CTKD), encargado de configurar claves de autenticación al emparejar dos dispositivos entre

sí.

Un peligro con solución… en camino

Al emparejar dos dispositivos Bluetooth se configuran dos conjuntos diferentes de claves de autenticación para el estándar de Bluetooth de baja energía (BLE) y de velocidad básica / velocidad de datos mejorada (BR / EDR). La función de CTKD es tener las claves listas y dejar que los dispositivos emparejados decidan qué versión del estándar Bluetooth quieren usar. Es aquí donde se ha detectado esta peligrosa vulnerabilidad.

Organismos como el SIG y el CERT alertan de que debido a este «fallo» detectado en el proceso, un atacante podría manipular el componente CTKD para sobrescribir otras claves de autenticación de Bluetooth en un dispositivo. De esta forma se le podría conceder permisos a un atacante para que se conecte a través de Bluetooth a otros servicios / aplicaciones compatibles con Bluetooth en el mismo dispositivo.

Lo más «peliagudo» es que, a día de hoy, todos los dispositivos que utilizan el estándar Bluetooth 4.0 a 5.0 son vulnerables a estos ataques y estas son las versiones más extendidas en nuestros teléfonos móviles. a cambio, aquellos smartphones comprados en los últimos meses que funcionen bajo el estándar Bluetooth 5.1, están libres del problema al contar con características que pueden prevenir ataques de este tipo.

La única forma de protegerse contra los ataques de BLURtooth es controlar el entorno en el que se emparejan los dispositivos Bluetooth, para evitar ataques man-in-the-middle, o emparejamientos con dispositivos poco confiables. No obstante ya se ha confirmado que se está trabajando en los parches que acaben con esta vulnerabilidad, con vistas a suministrarlos lo antes posible a los fabricantes par incluirlos como actualizaciones de firmware para los terminales afectados.

Para saber si tu teléfono está protegido contra este fallo y saber si has recibido un parche para los ataques BLURtooth, puedes comprobar la información presente en la versión del firmware y del sistema operativo de tu teléfono y localizar el identificador CVE-2020-15802 que pone fin a esta vulnerabilidad.

Fuente: movilzona.