Bluetooth SIG, la organización que supervisa el desarrollo de estándares de Bluetooth, emitió hoy una declaración en la que informa a los usuarios y proveedores sobre una vulnerabilidad sin parchear recientemente reportada, que potencialmente afecta a cientos de millones de dispositivos en todo el mundo.

Descubierto independientemente por dos equipos separados de investigadores académicos, la vulnerabilidad reside en la derivación de claves de transporte cruzado (CTKD) de dispositivos que admiten tanto el estándar de velocidad básica / velocidad de datos mejorada (BR/EDR), como de Bluetooth de baja energía (BLE).

La derivación de claves de transporte cruzado (CTKD) es un componente de Bluetooth responsable de negociar las claves de autenticación al emparejar dos dispositivos Bluetooth juntos, también conocidos como dispositivos de *«modo dual»*.

Nombrada como BLURtooth y rastreada como CVE-2020-15802, la falla expone los dispositivos con tecnología Bluetooth 4.0 o 5.0, lo que permite a los atacantes conectarse sin autorización a un dispositivo cercano objetivo sobrescribiendo la clave autenticada o reduciendo la fuerza de la clave de cifrado.

> *«Los dispositivos de modo dual que utilizan CTKD para generar claves de largo plazo (LTK) o clave de enlace (LK), pueden sobrescribir el LTK o LK original en los casos en que ese transporte imponía un nivel de seguridad más alto»,* dijeron los investigadores.
>
> *«Los dispositivos vulnerables deben permitir que un emparejamiento o enlace procesa de forma transparente sin autenticación, o con una fuerza de clave débil, en al menos uno de los transportes BR/EDR o LE para que sean susceptibles a un ataque».*

En otras palabras, la capacidad de aprovechamiento defectuosa bajo implementaciones

específicas del proceso de emparejamiento, podría permitir que los dispositivos sobrescriban las claves sin autorización cuando el transporte impone un nivel más alto de seguridad.

Según un aviso publicado por Carnegie Mellon CERT Coordination Center, la falla puede conducir a varios ataques potenciales, agrupados como *«ataques BLUR»*, incluido el ataque MitM.

> *«Si un dispositivo que falsifica la identidad de otro dispositivo se empareja o enlaza en un transporte y se usa CTKD para derivar una clave que luego sobrescribe una clave preexistente de mayor solidez o que se creó mediante autenticación, entonces puede ocurrir el acceso a servicios autenticados»,* advierte Bluetooth SIG.
>
> *«Esto puede permitir un ataque Man in the Middle (MitM) entre dispositivos previamente vinculados mediante emparejamiento autenticado cuando esos dispositivos pares son vulnerables»,* agregó.

Además de recomendar la introducción de restricciones en CTKD exigidas en las versiones 5.1 y posteriores de la especificación principal de Bluetooth como mitigación principal, Bluetooth SIG también se está coordinando con los fabricantes de dispositivos afectados para ayudarlos a lanzar los parches necesarios rápidamente.

> *«Bluetooth SIG recomienda además que los dispositivos restrinjan cuando se pueden emparejar en el transporte a los momentos en que la interacción del usuario coloca el dispositivo en un modo de emparejamiento o cuando el dispositivo no tiene enlaces o conexiones existentes a un dispositivo emparejado»,* dijeron los investigadores.