BLURTooth

CVSS: *Pending*

BLURtooth is a recently disclosed Bluetooth vulnerability [1] that affects numerous devices implementing dual-mode connectivity defined in the Bluetooth Core Specification, versions 4.2 through 5.0 [2]. Dual-mode connectivity represents a device capable of using Bluetooth Low Energy (BLE) and Bluetooth Classic (Basic Rate/Enhanced Data Rate or BR/EDR) transport layers. To facilitate this connectivity, the Bluetooth Core Specification defines the Cross-Transport Key Derivation (CTKD) protocol. The Bluetooth Special Interest Group (SIG) reports that researchers at the École Polytechnique Fédérale de Lausanne (EPFL) and Purdue University identified vulnerabilities explicitly related to CTDK [3].

The CTKD protocol is first described in the Bluetooth Core Specification v4.2 BR/EDR/LE Security Aspects [4]. The protocol enables dual-mode capable devices to generate two respective encryption keys upon pairing. Specifically, the devices need only to successfully connect over the LE or BR/EDR transport layer to get encryption keys for both layers. The specification refers to this as a "single pairing procedure" that provides a "better user experience." The type of key generated depends on the pairing procedure used. LE Secure Connection generates a 128-bit Long Term Key (LTK). The LTK is persistent and is an input to create a session key for encrypting the connection at the link layer. BR/EDR Secure Simple pairing generates a 128-bit Link Key (LK). The LK is persistent and encrypts the connection at the link layer.

Depending on which transport connection occurred first, the CTKD protocol may derive the LK from LTK, and vice-versa.

The CTKD protocol is vulnerable because it allows for a device pairing, under particular conditions, to overwrite an existing LTK or LK with a non-authenticated or weaker key. CERT describes the conditions as "vulnerable devices must permit a pairing or bonding to proceed transparently with no authentication, or a weak key strength, on at least one of the BR/EDR or LE transports," [5]. For example, devices A and B pair via LE Secure Connection using Passkey entry. Then, a malicious device C spoofs B and pairs to A using JustWorks over BR/EDR. The LTK shared between A and B is overwritten, as described above. Further, a man-in-the-middle attack is possible if both A and B are vulnerable.

In terms of attacker capability, the attacker needs to be within wireless range of the vulnerable devices (60-100m and potentially further with the proper antenna). The device also needs to support unauthenticated pairings and lack user-controlled access restrictions. This type of access restriction may include a notification for the user to view and approve.

Bluetooth SIG recommends that manufacturers either upgrade to the Bluetooth Core Specification v5.1 and later [3], and restrict when devices are pairable (i.e., when the user puts the device into a pairable mode) [5].

This vulnerability affects numerous IoT, smartphones, and embedded systems. It also impacts medical devices. For example, blood pressure monitors, CGMs, insulin pumps, infusion pumps, and patient health monitors are all medical devices that include Bluetooth functionality in their architecture and design. We found Bluetooth controllers such as Texas Instruments' CC2564C that support dual-mode and target medical devices [6][7]. Patient safety risks will have to be assessed by manufacturers, given that they may already implement the mitigations described by the Bluetooth SIG. However, manufacturers should consider upgrading to a controller or SoC that supports the latest Bluetooth Core Specification.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15802
[2] https://www.bluetooth.com/specifications/archived-specifications/
[3]https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/blurtooth/
[4] https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=441541
[5] https://www.kb.cert.org/vuls/id/589825/
[6]https://www.electronicspecifier.com/products/communications/dual-mode-bluetooth-device-for-pos-and-medical-devices
[7] https://www.ti.com/product/CC2564C