Application Report
Bluetooth® Low Energy, Basic Rate/Enhanced Data Rate – PIN-Code Pairing Key Derivation

TEXAS INSTRUMENTS

TI-PSIRT-2020-090070

CVEID: CVE-2020-26555

Publication date: May 27, 2021

Summary

A potential *Bluetooth*® protocol vulnerability impacts BR/EDR legacy PIN-code pairing, allowing a device pairing and connection without the actual PIN code. To do this, an attacker can connect to a device, claiming the device's own address and generating a random number value in the legacy pairing request reflected by an attacker to connect with a null combination key, regardless of the value of the PIN code or original key.

CVSS base score: 5.4

CVSS vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Affected products and versions

- CC2564C FW version v1.4
- WL18xx FW version v4.6

Potentially impacted features

Secure Simple Pairing or BR/EDR Secure Connections is sufficient to bypass this issue and no new FW or software is needed, as this is an option available today with higher security.

As with other reflection attacks, disallowing accepting the reflected value is sufficient to stop an attacker from proceeding with the PIN-code pairing attack. To address this, see mitigation releases below.

Suggested mitigations

The following software updates will address the potential vulnerability by disallowing reflection of the random number value. It is recommended that customers apply the software updates if legacy PIN-code pairing is used.

Affected SDK/FW	Version with mitigations	Release dates
CC2564C FW version v1.5	https://www.ti.com/tool/CC256XC-BT-SP	May 2021
WL18xx FW version v4.7	Available upon request: ti_bt_errata@list.ti.com	–

IMPORTANT NOTICE AND DISCLAIMER