

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



## 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	<a href="https://www.ti.com/tool/CC256XC-BT-SP">https://www.ti.com/tool/CC256XC-BT-SP</a>	May 2021
WL18xx FW version v4.7	Available upon request: <a href="mailto:ti_bt_errata@list.ti.com">ti_bt_errata@list.ti.com</a>	–

## IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to [TI's Terms of Sale](#) or other applicable terms available either on [ti.com](http://ti.com) or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265  
Copyright © 2022, Texas Instruments Incorporated