

Bluetooth® SIG Erratum – Authentication of the LE Legacy Pairing Protocol



TI-PSIRT-2020-100069

Publication date: May 23, 2021

Summary

A local attacker can insert itself during the pairing protocol of a central and a peripheral using LE Legacy Pairing and complete phase 2 of the authentication without knowledge of the temporary key (TK).

Affected products and versions

- CC2640R2 SDK, [BLE-STACK](#) (SDK v4.40.00.xx and prior versions)
- CC2640R2 SDK, [BLE5-STACK](#) (SDK 4.40.00.xx and prior versions)
- CC13X2-26X2-SDK, [BLE5-STACK](#) (SDK v4.40.00.44 and prior versions)
- [CC1350](#) SDK, [BLE-STACK](#) (SDK v4.10.xx and prior versions)
- CC26x0 [BLE-STACK](#) (v2.2.5 and prior versions)
- CC25x0 [BLE-STACK](#) (BLE-STACK 1.5.1 and prior versions)
- CC2564C TI Dual-Mode *Bluetooth* Stack (v4.2.1.1)
- WL18xx TI Dual-Mode *Bluetooth* Stack (v4.2.1.1)

Potentially impacted features The potential vulnerability can impact *Bluetooth*® Low Energy devices running affected SDK versions that have configured the devices as a *Bluetooth* Low Energy central and legacy pairing procedure is enabled. However, no loss of confidentiality or integrity happens unless the implementation is incorrectly using an un-encrypted link during pairing.

Suggested mitigations

The following SDK releases will address the potential vulnerability:

Affected SDK	SDK version with mitigations	SDK release dates with mitigations
CC2640R2 SDK, BLE-STACK	SDK v 5.10.00.02	April 2021
CC2640R2 SDK, BLE5-STACK		
CC13X2-26X2-SDK, BLE5-STACK	SDK v 5.10.00.48	April 2021
CC13x0 SDK, BLE-STACK	SDK v 4.20.00.05	April 2021
BLE-STACK (support for CC2640/CC2650)	BLE-STACK v2.2.6	April 2021
BLE-STACK (support for CC2540/CC2541)	BLE-STACK v1.5.2	May 2021
CC2564C TI Dual-Mode <i>Bluetooth</i> Stack	v4.2.1.2	May 2021
WL18xx TI Dual-Mode <i>Bluetooth</i> Stack	v4.2.1.2	May 2021

External references

[Bluetooth SIG Statement Regarding the 'Authentication of the LE Legacy Pairing' Vulnerability](#)

Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from May 23, 2021 to May 27, 2021	Page
• Added "External references" section.....	1

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 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