PSIRT Notification

Denial of Service during Bluetooth LE authentication and connection

1 Summary

An issue identified in the Texas Instruments Bluetooth® stack causes a Denial of Service (DoS) condition. The potential vulnerability can be exploited by sending a crafted LL_Pause_Enc_Req packet during the Bluetooth LE connection establishment phase. When processed by an affected device, this malformed packet can cause the device to enter an unresponsive state, requiring a manual reset to restore normal operation.

2 Vulnerability

TI PSIRT ID

TI-PSIRT-2025-070274

CVE ID

CVE-2025-44528

CVSS Score

The CVSS base score is 6.5.

Note

The CVSS scoring for this advisory considers the vulnerability as an adjacent attack vector, differing from the network attack vector listed in the CVEID

CVSS Vector

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

Affected Products

Part	Software Name	Software Version	BLE Stack Name	BLE Stack Version
CC2651P3, CC2651R3, CC2651R3SIPA, CC2642R, CC2652R, CC2652P, CC1352R, CC1352P, CC2652RSIP, CC2652PSIP, CC2642R-Q1, CC2652R7, CC2652P7, CC1352R7, CC1352P7	SIMPLELINK-CC13XX-CC26XX-SDK: SIMPLELINK-LOWPOWER-F2-SDK	SimpleLink™ CC13XX CC26XX SDK 7.41.00.17	BLE5-Stack	v2.2.8
CC2340R5, CC2340R5-Q1, CC2340R2	SIMPLELINK-LOWPOWER-F3-SDK	SimpleLink Low Power F3 SDK 9.10.00.00	BLE5-stack	v3.3.4
CC2745R10-Q1, CC2745R7-Q1, CC2744R7-Q1, CC2745P10-Q1, CC2755R10, CC2755P10	SIMPLELINK-LOWPOWER-F3-SDK	SimpleLink Low Power F3 SDK 9.10.00.00	BLE5-stack	v3.3.4
CC2640R2F, CC2640R2L, CC2640R2F-Q1	SIMPLELINK-CC2640R2-SDK: SimpleLink CC2640R2 SDK - Bluetooth low energy	SIMPLELINK-CC2640R2-SDK 5.30.01.11	BLE-Stack	v3.03.08.00 and earlier
			BLE5-Stack	v**1.01.14.00** and earlier
CC1350	SIMPLELINK-CC13X0-SDK: SimpleLink Sub-1GHz CC13x0 Software Development Kit	SIMPLELINK-CC13X0-SDK 4.20.02.07	BLE-Stack	v2.03.11.00 and earlier
CC2640, CC2650, CC2650MODA	N/A	2.02.08.12	BLE-STACK-2-X	v2.02.07.06 and earlier
CC2540, CC2541	N/A	1.05.02.00	BLE-STACK-1-X	v1.05.02.00 and earlier

Potentially Impacted Features

The potential vulnerability can impact TI Bluetooth Low Energy devices running the affected SDK versions with link layer encryption enabled and performing encryption operations during connection establishment, if implemented.

Suggested Mitigations

The following SDK releases addresses the potential vulnerability:

Affected SDK	First SDK Version with Mitigations	First BLE Stack Version with Mitigations
CC13XX-26XX-SDK, BLE5-STACK	SimpleLink Low Power F2 SDK 9.20.00.00	v3.4.0 (upcoming release)
CC2340 SDK, BLE5-STACK	SimpleLink Low Power F3 SDK 9.11.01.00	v3.3.4
CC27xx SDK, BLE5-STACK	SimpleLink Low Power F3 SDK 9.11.01.00	v3.3.4
CC2640R2 SDK, BLE5-STACK	In upcoming release	In upcoming release
CC2640R2 SDK, BLE-STACK	In upcoming release	In upcoming release
CC1350, CC26x0, CC25x0 SDK, BLE-STACK	N/A (1)	N/A(1)

(1) Mitigation on these device stacks is not supported as this is a fix to the BLE stack in devices' ROM, and with limited ROM patch space on these devices, the patch memory is being reserved for more critical PSIRT tickets in the future. If you have questions, please reach out to psirt@ti.com.

The software containing the mitigation described in this document can be distributed to already deployed devices through all enabled software update mechanisms, including Over-the-Air Download (OTA/OAD) update procedures.

References

- *Core Specification 5.3*. (2021, July 13). Bluetooth. Retrieved April 28, 2026 from https://www.bluetooth.com/specifications/specs/core-specification-5-3/
- Texas Instruments (2026). *Vulnerability Report: Premature Encryption Pause Attack on LP-CC2652RB* [Source code]. GitHub. https://github.com/yangting111/BLE_TEST/blob/main/result/PoC/TI/Accept_Pause_Enc_Req.md

Trademarks

SimpleLink™ is a trademark of Texas Instruments.
Bluetooth® is a registered trademark of Bluetooth SIG, Inc.
All trademarks are the property of their respective owners.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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 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, TI’s General Quality Guidelines, 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. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

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

Last updated 10/2025