PSIRT Notification

Bluetooth LE Secure Pairing Peripheral Devices Can Fail Connection With Central Devices

Summary

During Bluetooth LE secure pairing process, impacted devices operating in Bluetooth LE peripheral role can potentially enter a state where the devices cannot pair with central device leading to Denial of Service (DoS) attacks.

Vulnerability

TI PSIRT ID

TI-PSIRT-2022-090143

CVE ID:

None

CVSS Score

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

CVSS Base Score

2.6

Affected Products

Part	Software Name	Software version	TI BLE Stack Name	TI BLE Stack Version
CC2651P3, CC2651R3, CC2651R3SIPA, CC2642R, CC2652R, CC2652P, CC1352R, CC1352P, CC2652RSIP, CC2652PSIP, CC2642R-Q1, CC2652R7, CC2652P7, CC1312R7, CC1352P7	SIMPLELINK-CC13XX-CC26XX-SDK: SimpleLink™ CC13xx and CC26xx software development kit (SDK)	v6.41.00.17 and earlier	BLE5-Stack	v2.02.07.00 and earlier
CC2640R2F, CC2640R2L, CC2640R2F-Q1	SIMPLELINK-CC2640R2-SDK: SimpleLink™ CC2640R2 SDK - Bluetooth® low energy	v5.30.00.03 and earlier	BLE-Stack	v3.03.08.00 and earlier
			BLE5-Stack	v1.01.14.00 and earlier
CC1350	SIMPLELINK-CC13X0-SDK: SimpleLink™ Sub-1 GHz CC13x0 Software Development Kit	v4.20.02.07 and earlier	BLE-Stack	v2.03.11.00 and earlier
CC2640, CC2650, CC2650MODA	NA	NA	BLE-STACK-2-X	v2.02.07.06 and earlier
CC2540, CC2541	NA	NA	BLE-STACK-1-X	v1.05.02.00 and earlier

To determine if your product is impacted, check the version of the TI BLE stack version built into your product. This can be done by looking at the documentation included with SDK. Bluetooth LE products using only the peripheral role can be affected by this advisory during secure pairing process.

Potentially Impacted Features

When out of order packets are sent during Bluetooth LE secure pairing, the affected devices can be put in a state which results in the halting of any attempts to pair with other central devices. This state can lead to Denial of Service (DoS) attacks that can be recovered by resetting the device. This behavior was noticed with the following scenarios:

Scenario 1: Checks not performed on out of turn packets with pre-set value

During Bluetooth LE secure pairing, if the central sends *DHkeyCheckSend* message before sending *MackKey*, *Na* and *Nb*, the peripheral will respond with *DHkeyCheckSend* even though *MackKey*, *Na* and *Nb* are set to zero. During normal operation, *MackKey*, *Na* and *Nb* must be sent before *DHkeyCheckSend*.

Scenario 2: Bluetooth LE peripheral responds to out of turn packet before authentication

During Bluetooth LE secure pairing, a peripheral can respond out of turn to *PairRandomSend* message before *PublicKeySend* packet is received.

Scenario 3: Bluetooth LE peripheral responds to out of turn packet with incorrect value

During Bluetooth LE secure pairing, a peripheral can respond to *PairConfirmSend* request from a central with wrong confirm values set for *PairReq* with secure connection flag or OOB flag turned on. In this scenario, the *PairConfirmSend* packet is sent before *PublicKeySend* packet is received.

Suggested Mitigations

The following SDK releases addresses the potential vulnerability. Customers can upgrade to the latest SDK version to avoid this vulnerability.

Part	Software Name	Software version	TI BLE Stack Name	TI BLE Stack Version
CC2340R5, CC2340R5-Q1	SIMPLELINK-LOWPOWER-SDK: SimpleLink™ low power software development kits (SDKs)	v7.10.00.35	BLE5-Stack	v3.02.01.00
CC2651P3, CC2651R3, CC2651R3SIPA, CC2642R, CC2652R, CC2652P, CC1352R, CC1352P, CC2652RSIP, CC2652PSIP, CC2642R-Q1, CC2652R7, CC2652P7, CC1312R7, CC1352P7, CC2674R10, CC2674P10, CC1354R10, CC1354P10	SIMPLELINK-CC13XX-CC26XX-SDK: SimpleLink™ CC13xx and CC26xx software development kit (SDK)	v7.10.00.98	BLE5-Stack	v2.02.08.00
CC2640R2F, CC2640R2L, CC2640R2F-Q1	SIMPLELINK-CC2640R2-SDK: SimpleLink™ CC2640R2 SDK - Bluetooth® low energy	Not Supported[1]	BLE-Stack	Not Supported[1]
			BLE5-Stack	Not Supported[1]
CC1350	SIMPLELINK-CC13X0-SDK: SimpleLink™ Sub-1 GHz CC13x0 Software Development Kit	Not Supported[1]	BLE-Stack	Not Supported[1]
CC2640, CC2650, CC2650MODA	NA	Not Supported[1]	BLE-STACK-2-X	Not Supported[1]
CC2540, CC2541	NA	Not Supported[1]	BLE-STACK-1-X	Not Supported[1]

(1) Mitigations on these device stacks is not supported as this is a fix to the BLE stack in devices' ROM, which has a limited patch size. Given the severity of this issue is low, the patch memory is being reserved for critical PSIRT issues in the future.

External References

BLEDiff : *Scalable and Property-Agnostic Noncompliance Checking for BLE Implementations*, in 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, US, 2023 pp. 1082-1100.

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