PSIRT Notification

Bluetooth SIG Erratum - Incoming Notification/Indication Tests Upon Reconnection for GATT Client are Invalid

TI PSIRT ID

TI-PSIRT-2022-120154

Summary

A local attacker can insert itself during a reconnection between Bluetooth® LE GATT client and GATT server and succeed in sending indications or notifications to the GATT client even when the security requirements that were agreed upon during bonding is not met (for example, encryption with GATT server not enabled); thereby, compromising the security of the indications and notifications during a reconnection.

The GATT client tests per Bluetooth specification Version 5.3 and later, Vol3, Part C, Section 10.3.2.2 *Handling of GATT indications and notifications* does not check if IUT (Implementation Under Test) ignores notifications without establishing required security level *after* reconnection. Based on implementation, the GATT client can process indications and notifications from GATT server before the security requirements for the reconnection is met.

CVE ID

None

CVSS Score

5.7

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

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, 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	N/A	N/A	BLE-STACK-2-X	v2.02.07.06 and earlier
CC2540, CC2541	N/A	N/A	BLE-STACK-1-X	v1.05.02.00 and earlier

To determine if your product is impacted, check the version of the SimpleLink SDK and BLE stack built into your product. This can be done by looking at the documentation included with SDK.

Potentially Impacted Features

The potential vulnerability can impact Bluetooth® Low Energy devices (running the affected SDK versions) when configured as a Bluetooth Low Energy GATT Client using Bluetooth security modes and levels which require authentication and/or encryption in a connection with the bonded devices.

If the user application is using privacy for Bluetooth LE connections, then, the risk of this vulnerability is mitigated as only valid devices with known IRK (Identity Resolving Key) can establish connection / reconnection. Additionally, upon reconnection, if the GATT client is immediately increasing the security to the level agreed upon during bonding, the risks of this vulnerability is further mitigated.

Suggested Mitigations

The Bluetooth erratum changes propose GATT client role tests to be similar to their GATT server counterparts with the following steps:

- Bond
- Subscribe
- Disconnect
- Reconnect
- Ignore notifications/indications
- Enable security on link
- Process notifications

The following table lists the SDK releases with mitigations that addresses the potential vulnerability. If using impacted SDKs for which fixes are available, upgrade to the version of the SDK with fixes, or a later version.

Affected SDK	First SDK version with mitigations	First BLE stack version with mitigations
CC13XX-26XX-SDK, BLE5-STACK	SimpleLink™ CC13xx CC26xx SDK (7.10.00.98)	v2.02.08.00
CC2340 SDK, BLE5-STACK	SimpleLink™ Low Power F3 SDK (7.10.00.35)	v3.02.01.00
CC2640R2, CC1350, CC26x0, CC25x0 SDK, BLE-STACK	Not supported (1)	Not supported (1)
CC2640R2 SDK, BLE5-STACK	Not supported (1)	Not supported (1)

(1) Mitigation on these device stacks are 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

External References

1. Bluetooth Core Specification Revision v5.3 or later
2. Bluetooth SIG Statement *Incoming notification/indication tests for central role are invalid* erratum.
3. Texas Instruments, *Handling of GATT Indications and Notifications*

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