

TI Bluetooth: Invalid RPA Leading to DoS for Bonded Devices (CVE-2023-52709)



1 Summary

Bluetooth resolvable Random Private Address (RPA) enables mitigations towards malicious third-parties from tracking a Bluetooth device while still allowing one or more already bonded devices (trusted parties) to identify the Bluetooth device of interest. The RPA address is *resolvable* using a key (referred to as Identity Resolving Key - IRK) shared with the already bonded devices.

One of the Bluetooth LE fuzz tests causes the Bluetooth LE DUT (device under test) using RPA for connectable advertising, to end up generating unresolvable RPAs after a while. This leads to causing DoS for the already bonded peer devices until the next valid RPA is generated (15 minutes by default).

2 Vulnerability

TI PSIRT ID

TI-PSIRT-2023-08198

CVE ID

CVE-2023-52709

CVSS Base Score

6.5

CVSS Vector

[CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N](#)

Affected Products

Table 2-1. Affected Products

Device	Software Name	Software Version	BLE Stack Name	BLE Stack Version
CC2651P3, CC2651R3, CC2651R3SIPA, CC2642R, CC2642P, CC2652R, CC2652P, CC1352R, CC1352P, CC2652RSIP, CC2652PSIP, CC2642R-Q1, CC2652R7, CC2652P7, CC1352R7, CC1352P7	SIMPLELINK-CC13XX-CC26XX-SDK: SimpleLink™ software development kit (SDK)	V7.10.02.23 and earlier,	BLE5-Stack	v2.02.08.01 and earlier
CC2340R5, CC2340R5-Q1, CC230R2	SIMPLELINK-LOWPOWER-F3-SDK	v7.40.00.64 and earlier	BLE5-stack	v3.02.04.20 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-1GHz CC13x0 Software Development Kit	v4.20.02.07 and earlier	BLE-Stack	v2.03.11.00 and earlier
CC2640, CC2650, CC2650MODA	N/A	v2.02.07.06 and earlier	BLE-STACK-2-X	v2.2.7 and earlier
CC2540, CC2541	N/A	v1.05.02.00 and earlier	BLE-STACK-1-X	v1.5.2 and earlier

Potentially Impacted Features

The potential vulnerability can impact Bluetooth Low Energy devices running the affected SDK versions and enabled Bluetooth privacy with resolvable private address feature.

Suggested Mitigations

The following SDK releases addresses the potential vulnerability:

Table 2-2. Suggested Mitigations

Affected SDK	First SDK Version with Mitigations	First BLE Stack Version with Mitigations
CC13XX-26XX-SDK, BLE5-STACK	SIMPLELINK-LOWPOWER-F2-SDK (7.40.00.77)	v2.02.09.00
CC2340 SDK, BLE5-STACK	SimpleLink™ Low Power F3 SDK (8.10.00.55)	v3.03.01.00
CC2640R2 SDK, BLE5-STACK	SimpleLink™ CC2640R2 SDK 5.30.00.03	v1.01.15.00
CC2640R2 SDK, BLE-STACK	SimpleLink™ CC2640R2 SDK 5.30.00.03	v3.03.09.00
CC1350, CC26x0, CC25x0 SDK, BLE-STACK	N/A ⁽¹⁾	N/A ⁽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. For questions, see psirt@ti.com.

Acknowledgments

TI thanks Kevin Mitchell, from ETAS Inc., for reporting this vulnerability to TI PSIRT and working toward a coordinated disclosure.

External References

- [BLUETOOTH CORE SPECIFICATION](#), version 5.3
- [Bosch PSIRT Advisory](#)

Trademarks

SimpleLink™ is a trademark of Texas Instruments.

Bluetooth® is a registered trademark of Bluetooth Special Interest Group.

All trademarks are the property of their respective owners.

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](https://www.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 © 2024, Texas Instruments Incorporated