Application Note

Texas Instruments 802.15.4 Stack: Absence of Frame Counter Validation in SM Configuration

TI-PSIRT-2022-100125

Publication date: June 8, 2022

CVEID: None

Summary

Texas Instruments provides the TI 15.4-Stack implementing the IEEE 802.15.4e and 802.15.4g specifications. This stack is provided in several configurations, including an SM configuration. The SM configuration includes a “Secure Manager” which provides device commissioning services. The device commissioning service provided in this configuration is a custom service provided by Texas Instruments and it is not part of the IEEE standards. The use of this service is demonstrated in the Secure Commissioning example included with the TI 15.4-Stack.

The TI 15.4-Stack with Secure Manager did not include logic to check the frame counter of incoming packets as described in step h of section 9.2.4 of the IEEE 802.15.4-2020 standard. This allows attackers to capture network packets and resend those packets. The receiving device will process the packet as if it was sent by the original source of the packet.

CVSS base score: 4.3

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

Affected products and versions

Part	SDK	SDK Version	TI-15.4-Stack Version
CC2652RB, CC1311P3, CC1311R3, CC1312R7, CC1312R, CC1352P, CC1352P7, CC1352R, CC2651R3, CC2652P, CC2652P7, CC2652R, CC2652R7, CC2652PSIP, CC2652RSIP	SimpleLink™ CC13xx and CC26xx software development kit (SDK)	5.40.00.40 and earlier	4.40 and earlier

Because the impact is constrained to only the SM configuration, devices with an SDK that does not include the SM configuration are not impacted. Thus, the CC1310 and CC1350 devices are not impacted.

To determine if your product is impacted, check if the SM configuration of the library is built into your product. The SM configuration’s library is named maclib_sm_[device].a, where [device] is a SimpleLink device family designation. For example: maclib_sm_cc13x2.a or maclib_sm_cc26x1_2_4g.a. You may also check if your product’s development team started with the Secure Commissioning example project included in the SDK.

Potentially impacted features

The failure to correctly validate the frame counter may allow an attacker to replay network packets. The vulnerability does not allow an attacker to decrypt or modify packets.

Suggested mitigations

Customers are encouraged to upgrade to the latest SDK for their 802.15.4 product. After obtaining the latest SDK, customers should confirm a TI 15.4-Stack version of 5.10 or greater and upgrade their device to use the new version of the stack.

The following SDK releases address these vulnerabilities:

SDK	First SDK version with mitigations	First TI-15.4-Stack version with mitigations
SimpleLink™ CC13xx and CC26xx software development kit (SDK)	6.10	5.10.00

In addition, the MAC Comm Status Indication Callback may now receive an ApiMac_commStatusReason_rxSecure reason code when a frame is received with an unexpected frame counter. Customers may wish to update their callback's processing to handle this reason code. For example, customers may wish to log the occurrences of such an event. However, handling this new reason code is not required to achieve security or correct device operation.

Acknowledgment

We would like to thank Ryan Walker of TallyFi for reporting this vulnerability to the TI Product Security Incident Response Team (PSIRT).

External References

IEEE Std 802.15.4-2020, *IEEE Standard for Low-Rate Wireless Networks*, July 2020.

Revision history

- Version 1.0 Initial publication

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