Application Report

Bluetooth® Low Energy – Missing Length Check for UNPI Packets Over SPI on CC1350 and CC26x0 Devices

TI-PSIRT-2020-060056

Publication date: October 8, 2020

Summary

A local attacker able to interfere with the physical serial peripheral interface (SPI) bus between the host and the network processor may send a malformed uniformed network processor interface (UNPI) packet that can corrupt dynamic memory in the host processor, thus potentially achieving code execution.

CVSS base score: 7.6

CVSS vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Affected products and versions

- CC1350 SDK, BLE-STACK (SDK v4.10.01 and prior versions)
- CC26x0 BLE-STACK (v2.2.4 and prior versions)

Potentially impacted features

The potential vulnerability can impact *Bluetooth*® Low Energy devices running affected SDK versions that have configured the devices to run in network processor mode and uses UNPI with SPI transport layer as the serial interface between the *Bluetooth* Low Energy device and the external host processor.

Suggested mitigations

The following SDK releases address the potential vulnerability:

Affected SDK	SDK version with mitigations	SDK releases with mitigations
CC13x0 SDK, BLE-STACK	4.10.02	25-Aug-2020
BLE-STACK (support for CC2640 and CC2650)	BLE-STACK v2.2.5	31-Aug-2020

Acknowledgment

- Ruben Santamarta, IOActive

Revision history

- Version 1.0 initial publication

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, 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 (www.ti.com/legal/termsofsale.html) 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.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265