Application Report

Bluetooth Low Energy – Invalid Connection Request (SweynTooth)

TI-PSIRT-2019-100036

CVEID: CVE-2019-19193

Publication date: February 19, 2020

Summary

The Bluetooth® Low Energy peripheral implementation in our SimpleLink™ SDK and our dual-mode Bluetooth link layer can allow reception of the connection indication packet with invalid parameters. This can allow attackers in radio range to potentially crash the device via a crafted packet resulting in a denial of service.

Potential behavior in devices using SimpleLink SDK with BLE-STACK

When the Bluetooth Low Energy peripheral device receives an invalid connection PDU (invalid connection interval or supervision timeout parameters), a connection is attempted by the device. However, the connection does not succeed due to reception of invalid parameters. The connection fail status is indicated by the Bluetooth Low Energy stack to the application layer (bleGAPConnNotAcceptable). The “Simple Peripheral” example application that TI provides enters an idle state upon receiving the connection fail notification from the Bluetooth Low Energy stack and does not re-initiate advertisements again. This can potentially lead to a denial of service at an application level.

Potential behavior in devices using SimpleLink SDK with BLE5-STACK

When the Bluetooth Low Energy peripheral device receives an invalid connection PDU (invalid connection interval or supervision timeout parameters), the device RF core notifies the BLE5-STACK of the invalid condition and BLE5-STACK enters a hang condition. This could leads to a denial of service at an application level.

Potential behavior in devices using dual-model Bluetooth service pack

When the Bluetooth Low Energy peripheral device receives an invalid connection PDU (invalid connection interval or supervision timeout parameters), a connection is attempted by the device. The connection initially succeeds, but will later timeout due to the invalid parameters. Depending on the interval and timeout parameters settings from the connected remote device, a disconnection event is indicated to the host from the controller via HCI commands after the timeout period. During this period, essentially a denial of service is experienced, and the controller does not re-initiate advertisements again until a device reset occurs.

CVSS base score: 6.8

CVSS vector: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Affected products and versions

Here is the list of affected Bluetooth Low Energy SDKs:

BLE-STACK

- CC2640R2 SDK, BLE-STACK (SDK v3.30.00.20 and prior versions)
- CC25x0 BLE-STACK (BLE-STACK 1.5.0 and prior versions)
- CC1350 SDK, BLE-STACK (SDK v3.20.xx and prior versions)
- CC26x0 BLE-STACK (BLE-STACK v2.2.3 and prior versions)

BLE5-STACK

- CC2640R2 SDK, BLE5-STACK (SDK v3.30.00.20 and prior versions)
- CC13X2-26X2-SDK BLE5-STACK (SDK v3.40.00.02 and prior versions)

Dual-mode Bluetooth service pack

- Bluetooth service pack for CC256xC: CC256XC-BT-SP (v1.3 and earlier)
- Bluetooth service pack for CC256xB: CC256XB-BT-SP (v1.8 and earlier)

Potentially impacted features

The potential vulnerability can impact Bluetooth Low Energy devices running affected SDK versions that have configured the devices as a Bluetooth Low Energy peripheral and enabled connectable advertisements.

Suggested mitigations

The following service pack releases address the potential vulnerability:

Affected SDK	SDK version with mitigations	SDK releases with mitigations
CC2640R2 SDK BLE-STACK	SDK v3.40.00.10	09-Jan-2020
CC2640R2 SDK BLE5-STACK	SDK v.4.10.xx	08-Apr-2020
CC13X2-26X2-SDK, BLE5-STACK	SDK v4.10.xx	14-Apr-2020(1)
BLE-STACK (support for CC2540/CC2541)	v1.5.1	07-Feb-2020
CC13x0 SDK, BLE-STACK	SDK v4.10.xx	20-Mar-2020(1)
BLE-STACK (support for CC2640/CC2650)	BLE-STACK v2.2.4	16-Mar-2020(1)
Bluetooth service pack for CC256xC	V1.4	21-May-2020

(1) Consider subscribing to "Alert Me" at the corresponding SDK download links to be notified of the new SDK releases.

Note

For information on CC256X4B or other TI dual-mode Bluetooth devices that are not listed here, contact ti_bt_errata@list.ti.com.

External references

https://asset-group.github.io/disclosures/sweyntooth/

Revision history

- Version 1.0 initial publication
- Version 2.0 document type conversion

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