Application Report
Bluetooth low energy – Invalid Connection Request (SweynTooth)

TEXAS INSTRUMENTS

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.

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)

<u>BLE5-STACK</u>

- 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)

<u>Dual-mode Bluetooth service pack</u>

- Bluetooth service pack for CC256xC: CC256XC-BT-SP (v1.3 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.

External references

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

Trademarks
SimpleLink™ is a trademark of Texas Instruments.
Bluetooth® is a registered trademark of Bluetooth SIG, Inc.
All other trademarks are the property of their respective owners.

1 Revision History
NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from June 4, 2020 to July 28, 2020 (from Revision * (June 2020) to Revision A (July 2020))   **Page**
- Updated the numbering format for tables, figures and cross-references throughout the document...................1
- Remove CC256xB from the document..1

IMPORTANT NOTICE AND DISCLAIMER