Application Report

Bluetooth® Low Energy – Updating Connection MTU Size During an Ongoing OAD Operation May Cause Buffer Overflow

TI-PSIRT-2020-080063

Publication date: March 1, 2021

Summary

The TI *Bluetooth* ® Low Energy Over the Air Download (OAD) solution does not support updating Maximum Transmission Unit (MTU) size during an ongoing OAD operation, noted in our *Bluetooth* Low Energy stack user guide. If MTU size is updated during an OAD process, an attacker can cause buffer overflow that can potentially lead to remote code execution.

The proposed mitigation is to terminate the OAD process in case an MTU size exchange is done after the OAD process has started.

CVSS base score: 8.8

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

Affected products and versions

- CC2640R2 SDK, BLE-STACK (SDK v4.30.00.08 and prior versions)
- CC13X2-26X2-SDK BLE5-STACK (SDK v4.30.00.54 and prior versions)

Potentially impacted features

The potential vulnerability can impact *Bluetooth* Low Energy devices running affected SDK versions that use TI OAD sample applications, as no permissions are required for the peer to change MTU size.

Suggested mitigations

The following SDK releases address the potential vulnerability:

Affected SDK	SDK version with mitigations	SDK release dates with mitigations
CC2640R2 SDK BLE-STACK	SDK v 4.40.00.10	Feb 2021
CC13X2-26X2-SDK, BLE5-STACK	SDK v 4.40.00.44	Jan 2021

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