Application Note

低功耗蓝牙 - 无效的连接请求 (SweynTooth)

TI-PSIRT-2019-100036

CVEID: CVE-2019-19193

出版日期：2020 年 2 月 19 日

总结

低功耗 ***Bluetooth®*** 外围实现（位于 SimpleLink™ SDK）和我们的双模蓝牙链路层支持接收带有无效参数的连接指示数据包。这可能使无线电范围内的攻击者采用精心制作的数据包使设备崩溃，从而导致拒绝服务。

当低功耗蓝牙外围器件接收到无效的连接 PDU（无效的连接间隔或监督超时参数）时，该器件会尝试连接。但是，由于接收到无效参数，连接没有成功。低功耗蓝牙栈向应用层发送连接失败状态 (bleGAPConnNotAcceptable)。TI 提供的“简单外设”示例应用在收到来自低功耗蓝牙栈的连接失败通知后进入空闲状态，并且不会再次重新启动广播。这可能会导致应用级别的拒绝服务。

使用 SimpleLink SDK BLE5-STACK 的器件潜在行为

当低功耗蓝牙外围器件收到无效的连接 PDU（无效的连接间隔或监督超时参数）时，器件射频内核会将无效条件通知 BLE5-STACK，然后，BLE5-STACK 进入挂起状态。这可能会导致应用级别的拒绝服务。

使用双模型蓝牙服务包的器件潜在行为

当低功耗蓝牙外围器件接收到无效的连接 PDU（无效的连接间隔或监督超时参数）时，该器件会尝试连接。连接最初会成功，但稍后会因参数无效而超时。根据连接的远程器件的间隔和超时参数设置，超时之后，通过 HCI 命令从控制器向主机指示断开连接事件。在此期间，基本上会出现拒绝服务，并且控制器不会再次重新启动广播，直到器件复位。

CVSS 基础分数：6.8

CVSS 矢量： 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

受影响的产品和版本

以下是受影响的低功耗蓝牙 SDK 的列表：

BLE-STACK

- CC2640R2 SDK、BLE-STACK（SDK v3.30.00.20 及更早版本）
- CC25x0 BLE-STACK（BLE-STACK 1.5.0 及更早版本）
- CC1350 SDK、BLE-STACK（SDK v3.20.xx 及更早版本）
- CC26x0 BLE-STACK（BLE-STACK v2.2.3 及更早版本）

English Document: SWRA676
Copyright © 2021 Texas Instruments Incorporated

BLE5-STACK

- CC2640R2 SDK、BLE5-STACK（SDK v3.30.00.20 及更早版本）
- CC13X2-26X2-SDK BLE5-STACK（SDK v3.40.00.02 及更早版本）

双模蓝牙服务包

- 适用于 CC256xC 的蓝牙服务包：CC256XC-BT-SP（v1.3 及更早版本）

可能受影响的功能

该潜在漏洞可能会影响运行受影响 SDK 版本的低功耗蓝牙器件，这些 SDK 版本已将器件配置为低功耗蓝牙外围器件并启用了可连接广播。

建议的缓解措施

以下服务包版本解决了这个潜在的漏洞：

受影响 SDK	具有缓解措施的 SDK 版本	具有缓解措施的 SDK 版本
CC2640R2 SDK BLE-STACK	SDK v3.40.00.10	2020 年 1 月 9 日
CC2640R2 SDK BLE5-STACK	SDK v.4.10.xx	2020 年 4 月 8 日
CC13X2-26X2-SDK、BLE5-STACK	SDK v4.10.xx	2020 年 4 月 14 日(1)
BLE-STACK（支持 CC2540/CC2541）	v1.5.1	2020 年 2 月 7 日
CC13x0 SDK、BLE-STACK	SDK v4.10.xx	2020 年 3 月 20 日(1)
BLE-STACK（支持 CC2640/CC2650）	BLE-STACK v2.2.4	2020 年 3 月 16 日(1)
适用于 CC256xC 的蓝牙服务包	V1.4	2020 年 5 月 21 日

(1) 考虑在相应的 SDK 下载链接上订阅“通知我”，以获取有关新 SDK 版本的通知。

外部参考文献

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

商标

SimpleLink™ is a trademark of Texas Instruments.
Bluetooth® is a registered trademark of Bluetooth SIG, Inc.
所有商标均为其各自所有者的财产。

1 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from JUNE 4, 2020 to JULY 28, 2020 (from Revision * (June 2020) to Revision A (July 2020)) **Page**

- 更新了整个文档中的表格、图和交叉参考的编号格式 1
- 删除了文档中的 CC256xB 1

English Document: SWRA676
Copyright © 2021 Texas Instruments Incorporated

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2022，德州仪器 (TI) 公司