Application Note

低功耗 Bluetooth® – 有关 CC1350 和 CC26x0 器件通过 SPI 发送的 UNPI 数据包缺失长度检查

TI-PSIRT-2020-060056

出版日期：2020 年 10 月 8 日

总结

能够干扰主机和网络处理器之间的物理串行外设接口 (SPI) 总线的本地攻击者可能会发送格式错误的统一网络处理器接口 (UNPI) 数据包，该数据包可能会破坏主机处理器中的动态存储器，从而可能实现代码执行。

CVSS 基础分数：7.6

CVSS 矢量： 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

受影响的产品和版本

- CC1350 SDK、BLE-STACK（SDK v4.10.01 及更早版本）
- CC26x0 BLE-STACK（v2.2.4 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 *Bluetooth*® 器件，这些版本已将器件配置为在网络处理器模式下运行，并使用带 SPI 传输层的 UNPI 作为低功耗*蓝牙*器件和外部主机处理器之间的串行接口。

建议的缓解措施

以下 SDK 版本解决了该潜在漏洞：

受影响的 SDK	具有缓解措施的 SDK 版本	具有缓解措施的 SDK 版本的发行日期
CC13x0 SDK、BLE-STACK	4.10.02	2020 年 8 月 25 日
BLE-STACK（支持 CC2640 和 CC2650）	BLE-STACK v2.2.5	2020 年 8 月 31 日

确认

- IOActive 的 Ruben Santamarta

修订历史记录

- 初始发布版本 1.0

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