PSIRT Notification

德州仪器 (TI) Wi-SUN® 堆栈：帧计数器验证缺失

总结

德州仪器 (TI) 提供了采用 IEEE® 802.15.4g 规范的 Wi-SUN® 堆栈。TI Wi-SUN® 堆栈不包含用于检查传入数据包帧计数器的逻辑，如 IEEE® 802.15.4-2020 标准 9.2.3 节的步骤 h 所述。这使得攻击者可以捕获网络数据包并重新发送这些数据包。接收器件会将这些数据包作为由原始源发送的数据包进行处理。

漏洞

TI PSIRT ID

TI-PSIRT-2022-100128

CVE ID：

无

CVSS 分数

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS 基础分数：

4.3

受影响的产品

器件	SDK	SDK 版本	TI-Wi-SUN-Stack 版本
CC1352R、CC1352P7、CC1352P、CC1312R7、CC1312R、CC1200	SIMPLELINK-CC13XX-CC26XX-SDK：SimpleLink™ CC13xx 和 CC26xx 软件开发套件(SDK)	6.40.00.13 及更早版本	1.0.6 及更早版本

要确定您的产品是否受到影响，请检查产品中内置的 TI Wi-SUN® 堆栈版本。可以通过查看 SDK 附带的文档进行检查。

可能受影响的功能

如果未能正确验证帧计数器，攻击者可能会重放网络数据包。此漏洞不允许攻击者解密或修改数据包。

建议的缓解措施

我们建议客户升级到其 Wi-SUN® 产品的最新 SDK。获得最新的 SDK 后，客户应确认 TI Wi-SUN® 堆栈版本为 2.10.00 或更高版本，并将其器件升级为使用新版本的堆栈。

以下 SDK 版本解决了这些漏洞：

SDK	首个具有缓解措施的 SDK 版本	首个具有缓解措施的 TI-Wi-SUN-Stack 版本
SIMPLELINK-CC13XX-CC26XX-SDK：SimpleLink™ CC13xx 和 CC26xx 软件开发套件(SDK)	7.10	2.10.00

外部参考文献

IEEE® Std 802.15.4-2020, *IEEE Standard for Low-Rate Wireless Networks*, July 2020.

Wi-SUN® Alliance, Technical Profile Specification Field Area Network, Version 1v33

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