PSIRT Notification

低功耗蓝牙安全配对外设可能无法与中央器件连接

总结

在低功耗蓝牙安全配对过程中，以低功耗蓝牙外设角色运行的受影响器件可能会进入一种无法与中央器件配对的状态，从而导致拒绝服务 (DoS) 攻击。

漏洞

TI PSIRT ID

TI-PSIRT-2022-090143

CVE ID：

无

CVSS 分数

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

CVSS 基础分数

2.6

受影响的产品

器件	软件名称	软件版本	TI BLE 栈名称	TI BLE 栈版本
CC2651P3、CC2651R3、CC2651R3SIPA、CC2642R、CC2652R、CC2652P、CC1352R、CC1352P、CC2652RSIP、CC2652PSIP、CC2642R-Q1、CC2652R7、CC2652P7、CC1352R7、CC1352P7	SIMPLELINK-CC13XX-CC26XX-SDK：SimpleLink™ CC13xx 和 CC26xx 软件开发套件(SDK)	v6.41.00.17 及更早版本	BLE5-Stack	v2.02.07.00 及更早版本
CC2640R2F、CC2640R2L、CC2640R2F-Q1	SIMPLELINK-CC2640R2-SDK：SimpleLink™ CC2640R2 SDK - 低功耗 Bluetooth®	v5.30.00.03 及更早版本	BLE-Stack	v3.03.08.00 及更早版本
			BLE5-Stack	v1.01.14.00 及更早版本
CC1350	SIMPLELINK-CC13X0-SDK：SimpleLink™ Sub-1GHz CC13x0 软件开发套件	v4.20.02.07 及更早版本	BLE-Stack	v2.03.11.00 及更早版本
CC2640、CC2650、CC2650MODA	不适用	不适用	BLE-STACK-2-X	v2.02.07.06 及更早版本
CC2540、CC2541	不适用	不适用	BLE-STACK-1-X	v1.05.02.00 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 BLE 栈版本。可以通过查看 SDK 附带的文档进行检查。在安全配对过程中仅使用外设角色的低功耗蓝牙产品可能会受到此公告的影响。

English Document: SWRA783

可能受影响的功能

在低功耗蓝牙安全配对期间发送错序数据包时，受影响的器件可能会进入某种状态，导致任何与其他中央器件配对的尝试都停止。该状态可能会导致拒绝服务 (DoS) 攻击，通过复位器件即可恢复。以下场景中会出现这种行为：

场景 1：未使用预设值对错序数据包执行检查

在低功耗蓝牙安全配对期间，如果中央器件在发送 *MackKey*、*Na* 和 *Nb* 之前发送 *DHkeyCheckSend* 消息，即使 *MackKey*、*Na* 和 *Nb* 设置为零，外设也会以 *DHkeyCheckSend* 响应。正常工作期间，必须在 *DHkeyCheckSend* 之前发送 *MackKey*、*Na* 和 *Nb*。

场景 2：低功耗蓝牙外设在身份验证之前响应错序数据包

在低功耗蓝牙安全配对期间，外设在收到 *PublicKeySend* 数据包之前，会错序响应 *PairRandomSend* 消息。

场景 3： 低功耗蓝牙外设使用不正确的值响应错序数据包

在低功耗蓝牙安全配对期间，外设会在开启安全连接标志或 OOB 标志的情况下，使用为 *PairReq* 设置的错误确认值响应来自中央器件的 *PairConfirmSend* 请求。这种情况下，会在收到 *PublicKeySend* 数据包之前发送 *PairConfirmSend* 数据包。

建议的缓解措施

以下 SDK 版本解决了该潜在漏洞。客户可以升级到最新 SDK 版本以避免该漏洞。

器件	软件名称	软件版本	TI BLE 栈名称	TI BLE 栈版本
CC2340R5、CC2340R5-Q1	SIMPLELINK-LOWPOWER-SDK：SimpleLink™ 低功耗软件开发套件 (SDK)	v7.10.00.35	BLE5-Stack	v3.02.01.00
CC2651P3、CC2651R3、CC2651R3SIPA、CC2642R、CC2642P、CC2652R、CC2652P、CC1352R、CC1352P、CC2652RSIP、CC2652PSIP、CC2642R-Q1、CC2652R7、CC2652P7、CC1352R7、CC1352P7、CC2674R10、CC2674P10、CC1354R10、CC1354P10	SIMPLELINK-CC13XX-CC26XX-SDK：SimpleLink™ CC13xx 和 CC26xx 软件开发套件(SDK)	v7.10.00.98	BLE5-Stack	v2.02.08.00
CC2640R2F、CC2640R2L、CC2640R2F-Q1	SIMPLELINK-CC2640R2-SDK：SimpleLink™ CC2640R2 SDK - 低功耗 Bluetooth®	不支持 [1]	BLE-Stack	不支持 [1]
			BLE5-Stack	不支持 [1]
CC1350	SIMPLELINK-CC13X0-SDK：SimpleLink™ Sub-1GHz CC13x0 软件开发套件	不支持 [1]	BLE-Stack	不支持 [1]
CC2640、CC2650、CC2650MODA	不适用	不支持 [1]	BLE-STACK-2-X	不支持 [1]
CC2540、CC2541	不适用	不支持 [1]	BLE-STACK-1-X	不支持 [1]

(1) 不支持对这些器件栈进行缓解，因为这是针对补丁大小有限的器件 ROM 中 BLE 栈的修复。鉴于该问题的严重性较低，补丁存储器将保留用于处理未来的重要 PSIRT 问题。

外部参考文献

BLEDiff：*Scalable and Property-Agnostic Noncompliance Checking for BLE Implementations*，2023 年 IEEE 安全与隐私研讨会 (SP)，美国加利福尼亚州旧金山，2023 年，第 1082-1100 页。

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