Application Note

SimpleLink™ 器件的变量时间标签比较

TI-PSIRT-2019-080030

出版日期：2020 年 2 月 28 日

总结

签名验证实现方案使用一个非常量时间函数 memcmp，导致 MAC 检查可能容易受到计时攻击。

CVSS 基础分数：7.5

CVSS 矢量： https://www.first.org/cvss/calculator/3.0

受影响的产品和版本

- CC26X0
- CC13X0
- CC2640R2
- CC26X2
- CC13X2
- MSP432E4
- CC32XX

可能受影响的功能

- CC26X0、CC13X0：AES CCM
- CC26X2、CC13X2：AES CCM、AES GCM、ECDSA、ECJPAKE
- MSP432E4：AES CCM、AES GCM
- CC32XX：HMAC

建议的缓解措施

以下服务包版本解决了这个潜在的漏洞：

受影响的 SDK	具有缓解措施的 SDK 版本
SimpleLink CC13x2-26x2-SDK	3.30.00.03 及更高版本
SimpleLink MSP432E4 SDK	3.30.00.22 及更高版本
SimpleLink CC32xx SDK	3.30.00.04 及更高版本
SimpleLink CC13x0 SDK	4.10.00.10 及更高版本
SimpleLink CC2640R2 SDK	4.10.00.10 及更高版本

致谢

- TI 内部发现人员

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