Application Report

低功耗蓝牙、基本速率/增强型数据速率 – 方法混淆配对漏洞

TI-PSIRT-2020-020038

CVEID: CVE-2020-10134

出版日期：2020 年 5 月 18 日

总结

根据慕尼黑工业大学 (TUM) 研究人员关于一潜在安全漏洞的研究发现，Bluetooth® 特别兴趣组 (SIG) 发出提醒，该漏洞使攻击设备具备在两个配对设备之间发起中间人攻击的能力。为此，攻击者必须与一个设备协商数字比较过程，与另一个设备协商密钥配对过程，同时用户必须错误地输入数字比较值作为密钥，并在数字比较设备上接受配对。

可能受影响的功能

攻击设备需要位于两个易受攻击的蓝牙设备的无线范围内，该蓝牙设备通过密钥输入或数字比较建立 LE 或 BR/EDR 加密连接，以便在不具备现有共享凭据（LTK 或链接密钥）的情况下进行设备身份验证。至少一个设备必须允许密钥输入，另一个设备必须支持能够表示六位十进制数字的显示器。

建议的缓解措施

所有支持 BluetoothLE Secure Connections Pairing 和 Secure Simple Pairing 的设备均可能易受此攻击。Bluetooth SIG 提出可在应用层实现的建议。详情请参阅 Bluetooth SIG notice regarding the Method Confusion pairing vulnerability（蓝牙 SIG 关于方法混淆配对漏洞的通知）。

外部参考文献

- Bluetooth SIG notice regarding the Method Confusion pairing vulnerability（蓝牙 SIG 关于方法混淆配对漏洞的通知）
- CVE-2020-10134
- 慕尼黑工业大学 (TUM)

修订历史记录

- 初始发布版本 1.0

重要声明和免责声明

TI 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安全、安保或其他要求。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 (https:www.ti.com.cn/zh-cn/legal/termsofsale.html) 或 ti.com.cn 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。

邮寄地址：上海市浦东新区世纪大道 1568 号中建大厦 32 楼，邮政编码：200122