安全公告

标题	BLUFFS 经典蓝牙安全漏洞
发布日期	2024/01/18
公告编号	AR2023-010
编号	CVE-2023-24023
版本	V1.0

问题小结

BLUFFS （Bluetooth Forward and Future Secrecy Attacks and Defenses) 是由作者 **Daniele Antonioli** 公布的安全报告，被蓝牙联盟组织 (Bluetooth SIG) 编号为 CVE-2023-24023。BLUFFS 通过中间人（MITM）攻击经典蓝牙已配对设备间的传统安全连接（Legacy Secure Connection, LSC）加密会话；对于安全连接 (Secure Connection, SC) 加密会话，该漏洞则使用蓝牙冒充攻击 (BIAS) 方法，使 SC 降级为 LSC，并通过角色互换绕过认证过程。此外，BLUFFS 还会利用加密密钥协商攻击 (KNOB) 方法降级会话密钥的强度，以增大暴力破解加密密钥的成功率。攻击者在暴力破解加密密钥的同时，可以将会话数据保存下来，一旦密钥破解成功，之前保存下来的会话数据即可被破解。而在后续的加密会话建立过程中，BLUFFS 则利用经典蓝牙 LSC 加密密钥派生算法设计上的缺陷，强制会话使用已经破解后的密钥，因此会话中的数据也会被轻松破解。Bluetooth SIG 在其安全公告中指出该漏洞广泛存在于遵循蓝牙 4.2 至 5.4 核心规范的设备中，而其目前也只是提出了一些减弱该漏洞影响的措施，并未提出根本解决方案。

影响分析

前面已经提到， BLUFFS 的攻击对象是经典蓝牙已配对设备间的 LSC 加密会话，目前乐鑫受影响的芯片只有 ESP32 系列。由于 BLUFFS 漏洞属于协议层面上的缺陷，所以目前维护的 ESP-IDF 所有 Release 分支都会受到其影响。在 Bluetooth SIG 给出问题的根本解决方案前，拒绝会话 SC 降级和保证足够强的加密密钥强度都能有效减弱 BLUFFS 的攻击影响。

针对 BLUFFS ESP32 目前已实施的措施有：

1. KNOB 漏洞修复。 KNOB 漏洞补丁限制了 LSC 中的最小密钥强度为 7 字节长度，在该密钥强度下，攻击者很难实时破解会话加密密钥。该补丁在当前维护的 ESP-IDF Release 分支中都已经存在 (v4.3 ~ v5.2, master)。

2. BIAS 漏洞修复。相关信息可参考乐鑫安全公告 AR2021-004。 BIAS 漏洞补丁是在 ESP-IDF Bluedroid 协议栈中加入了防止对方降级安全连接的逻辑，对于经典蓝牙安全连接而言，ESP32 并未提供相关配置选项或接口。同时，该补丁也要求对方设备至少进行一次认证，这使得攻击者很难绕过认证过程，增加了攻击的难度。

ESP-IDF BIAS 漏洞问题版本

ESP-IDF Branch	Affected Commit ID	Affected IDF Version
master	042fd5f8 之前所有 commit	NA
release/v5.0	650b6653 之前所有 commit	v5.0
release/v4.4	07518cf4 之前所有 commit	v4.4~v4.4.3
release/v4.3	60e28180 之前所有 commit	v4.3~v4.3.4

ESP-IDF BIAS 漏洞修复版本

ESP-IDF Branch	Fixed Commit ID	Fixed IDF Version
master	042fd5f8	NA
release/v5.1	042fd5f8	v5.1
release/v5.0	650b6653	v5.0.1
release/v4.4	07518cf4	v4.4.4
Release/v4.3[1]	60e28180	v4.3.5

[1] ESP-IDF v4.3 已正式停止维护，乐鑫将不再对该版本提供增加新功能、修复 bug、修复安全问题等支持。

后续计划实施的措施有：

乐鑫将提供 API 来配置设备的最小密钥长度，对于安全需求较高的用户，可配置使用更高强度的加密会话密钥，提高暴力破解的时间和成本。

给使用者的建议

对 ESP32 系列产品进行开发及应用或需要从之前版本升级时，建议您使用上文中给出的 ESP-IDF 修复 Commit 之后的版本。如您在升级过程中遇到问题，请您反馈目前在用的 ESP-IDF 版本或 Commit ID 信息至乐鑫，乐鑫会尽快与您确认处理相关事宜。