安全公告

标题	有关“绕过 Wi-Fi 验证漏洞”的安全公告
发布日期	2023/11/03
公告编号	AR2020-002
编号	CVE-2020-12638
版本	V1.1

问题小结

当一个 ESP32 或 ESP8266 系统级芯片连接到加密的 Wi-Fi 接入点时，攻击者如注入一个伪造的 Wi-Fi 信标帧模拟接入点，可以导致芯片切换到开放认证模式。

芯片在受到攻击期间（即攻击者持续发送伪造信标帧期间），将不能继续与加密接入点进行通信。在此期间，芯片的身份验证模式将在开放和加密之间切换。然后，攻击者可以选择发送一个伪造的通道切换声明 (Channel Switch Announcement)，从而使芯片与一个新的通道建立关联 (Association)，并以开放身份验证模式与一个新的接入点保持连接。

该攻击的影响将导致系统级芯片传输一些未加密的 Wi-Fi 帧，或与受攻击者控制的开放接入点建立关联，允许未授权访问真正 Wi-Fi 接入点的攻击者访问 TCP/IP 层。

该攻击不允许攻击者绕过网络层的保护机制，如 TLS。该攻击也不允许攻击者获得对真正加密的 Wi-Fi 接入点的任何访问。

这个问题是由 Lukas Bachschwell 发现并向乐鑫披露的。Bachschwell 先生还注册了 CVE 编号：CVE-2020-12638。乐鑫在此感谢 Bachschwell 先生以负责任地态度对该问题进行了披露。

修复

ESP32

这个问题已经在 ESP-IDF v3.2.4 版本中得到修复，并在 v3.1.8，v3.3.3，v4.0.2，v4.1 和 v4.2 及之后版本中得到修复。

以下 IDF 分支均已经包含此次修复：
master: commit 0dba9329
release/v4.2: commit ad5c4eb3
release/v4.1: commit b6e2163e
release/v4.0: commit 68b272f5
release/v3.3: commit 4891fcea
release/v3.2: commit a5c8cdd3
release/v3.1: commit a280fb32

有关 ESP-IDF 发布分支和稳定发布版本的解释，请参阅 ESP-IDF 文档。

ESP8266

以下 ESP8266 RTOS SDK 中均包含此次修复：
master: commit da3362ec
release/v3.4: commit da3362ec
release/v3.3: commit 9c72c21b
release/v3.2: commit 3cbc3d87
release/v3.1: commit 4b1ff5c3
release/v3.0: commit 6ef5c2c2
release/v2.1: commit db188200

该问题也已在 ESP8266 NON-OS SDK 分支 be2f86d3 上进行修复。

ESP32-S2

release/v4.2 和 master 分支都包括了对这个问题的修复。ESP-IDF v4.2（即首个支持 ESP32-S2 的稳定发布版本）及之后版本不会受到这个问题的影响。

对使用乐鑫 Wi-Fi 设备者的建议

如果您的固件应用程序使用网络传输层安全协议（如 TLS），则受到的直接影响较低。但是，仍建议您立即更新到最新的稳定 ESP-IDF 版本或包含相关修复的 bug fix 版本。

如果您的固件应用程序并未使用 TLS 等网络传输层安全功能来保护重要数据，则应该考虑紧急升级到预发布的 ESP-IDF 或相关 SDK 版本，或升级到最新的稳定版本。

审查所有固件应用程序，确保所有敏感数据均已通过 TLS 或类似安全传输协议传输，并确保 TLS 配置正确，从而防止来自处于同一网络的攻击者的攻击。
审查所有固件应用程序，以确保设备提供的任何网络服务均会在进行任何受信功能前先验证网络客户端。如果服务会接收任何证书，则应该使用安全协议（如 TLS ）来传输这些证书。

修订历史

日期	版本	发布说明
2023/11/03	V1.1	更正章节 *修复* 中的修复信息。
2020/07/23	V1.0	首次发布。