安全公告

标题	有关 WFA 漏洞的安全公告
发布日期	2023/08/25
公告编号	AR2021-003
编号	CVE-2020-24586 CVE-2020-24587 CVE-2020-24588 CVE-2020-26146 CVE-2020-26147
版本	V1.1

问题小结

最近，Mathy Vanhoef 在其研究论文“分片与聚合：通过帧聚合和分片机制攻击 Wi-Fi 安全”(Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation) 中披露了一系列影响 Wi-Fi 设备的安全漏洞，其中包括三个标准设计缺陷和九个实现漏洞。更多有关这些漏洞的信息，请见这里。

我们发现，乐鑫设备可能受到本次披露中以下漏洞的影响：

- Wi-Fi 标准设计缺陷:

1) CVE-2020-24586: 分片缓存攻击（当[重新]连接到网络时，不从内存中清除片段）。
2) CVE-2020-24587: 混合密钥攻击（重组在不同密钥下加密的片段）。
3) CVE-2020-24588: 聚合攻击（接受 non-SPP A-MSDU 帧）。

- Wi-Fi 实现漏洞：

1) CVE-2020-26146: 重组非连续的加密片段。
2) CVE-2020-26147: 重组混合加密/明文片段。

攻击者可利用这些漏洞造成信息泄漏等后果。不过，为了实施攻击，攻击者必须成功注入 802.11 数据包，完成 MITM 攻击，并重定向到攻击者的恶意服务器。以上步骤缺一不可，因此在现实环境中通常很难实现。

请注意，这些攻击无法绕过 TLS 等网络层安全特性。

ESP-IDF 修复版本

ESP-IDF 分支	ESP-IDF 修复版本	修复 Commit ID
master	NA	ef127ab9
release/v4.3	v4.3.1	46144f70
release/v4.2	v4.2.3	60ccb3fe
release/v4.1	v4.1.2	97c8be71
release/v4.0	v4.0.4	7504329e
release/v3.3	v3.3.6	b403b0db

ESP8266 SDK 修复版本

ESP8266 SDK 分支	修复 Commit ID
master	08e225dd
release/v3.4	967752e2

有关使用乐鑫 Wi-Fi 设备的建议

如果您的固件应用程序使用了 TLS 等网络传输层安全功能，则直接受到本次披露漏洞的影响很小。使用 HTTPS 协议进行网络链接受到的直接影响也很低。另外，（如果有条件）使用 PMF (802.11w)、WPA3 和 EAP-TLS 可以进一步增强设备的安全性，使其免受 MITM 攻击。然而，您仍应在我们发布问题修补后，第一时间更新至带有问题修补的最新稳定 ESP-IDF 或 SDK 版本。
如果您的固件应用程序未使用 TLS 等网络传输层安全功能来保护重要数据，或者未使用最新的 Wi-Fi 安全协议（如 PMF/WPA3），则应考虑紧急更新到预发布版本或最新稳定版本的 ESP-IDF 或 SDK。

审阅所有固件应用程序，以确保所有敏感数据均已通过 TLS 或类似协议传输，并验证 TLS 配置是否正确。

审阅所有固件应用程序，以确保设备不会被任何方式引导至访问未知网站，并确保总使用 HTTPS 协议访问任何网站。

修订历史

日期	版本	发布说明
2023/08/25	V1.1	1. 修改 AR2021-003 的格式，将英文版本和中文版本分开； 2. 更新章节*问题小结*， ESP-IDF *修复版本*和 ESP8266 SDK *修复版本*的信息。
2021/06/25	V1.0	首次发布。