安全公告

标题	有关 WLAN FragAttacks 漏洞的安全公告
发布日期	2024/05/10
公告编号	AR2023-008
编号	CVE-2020-26142
版本	V1.1

问题小结

FragAttacks 是于 2021 年 5 月公开的一组 CVE 漏洞，涉及基于 WLAN 分段和/或 AMPDU 使用的 Wi-Fi 设备 MITM 攻击。

我们在乐鑫设备上发现了以下 Wi-Fi 实现漏洞：

受到影响的乐鑫 WLAN 设备会将每个 AMPDU 分段帧作为独立的完整帧处理，并且可能将其传递到应用层。这是一种 MITM 攻击，MITM 攻击者通过伪装其中一个分段帧，从而控制 WLAN 设备加载恶意 URL。

影响分析

这一漏洞将影响不涉及传输层安全措施的使用情景，例如使用 HTTP 协议加载 URL。

然而，攻击无法绕过网络层的传输层安全措施，例如使用 HTTPS 协议加载 URL。

影响产品系列

ESP8266、ESP32、ESP32-S2、ESP32-C2、ESP32-S3、ESP32-C3、ESP32-C6

影响 ESP8266 RTOS SDK 版本

ESP8266 RTOS SDK 分支	影响 commit ID	影响 ESP8266 RTOS SDK 版本
master	816bf9bc 之前所有 commit	/
release/v3.4	d47d0f4d 之前所有 commit	release/v3.4

影响 ESP-IDF 版本

ESP-IDF 分支	影响 commit ID	影响 ESP-IDF 版本
master	7ae8e1c4 之前所有 commit	/
release/v5.2	89dcaf4a 之前所有 commit	v5.2
release/v5.1	70f1bd58 之前所有 commit	v5.1 - v5.1.2
release/v5.0	5402e14c 之前所有 commit	v5.0 - v5.0.4
release/v4.4	629c3b4d 之前所有 commit	v4.4 - v4.4.6
release/v4.3	37b1fc9d 之前所有 commit	v4.3 - v4.3.6

应对方法

ESP8266 RTOS SDK 修复版本

ESP8266 RTOS SDK 分支	修复 commit ID	修复 ESP8266 RTOS SDK 版本
master	816bf9bc	/
release/v3.4	d47d0f4d	release/v3.4

ESP-IDF 修复版本

ESP-IDF 分支	修复 commit ID	ESP-IDF 修复版本
master	7ae8e1c4	/
release/v5.2	89dcaf4a	在 v5.2.1 修复
release/v5.1	70f1bd58	在 v5.1.3 修复
release/v5.0	5402e14c	在 v5.0.5 修复

release/v4.4	629c3b4d	在 v4.4.7 修复
release/v4.3	37b1fc9d	在 v4.3.7 修复

给应用程序开发者的建议

在使用乐鑫 WLAN 产品进行部署时，为了保障数据安全和防御相关攻击，请参考如下建议：

1. 如果网络层 TLS 被禁用，建议重新启用并升级到最新的稳定 ESP-IDF 版本。
2. 如果应用程序或 WLAN 网络禁用 PMF 或 WPA3，建议重新启用以增强数据链路层安全性。
3. 确保使用 HTTPS 连接所有网站，请勿提供绕过 HTTPS 的选项。

修订历史

日期	版本	发布说明
2024/05/10	V1.1	更新 *ESP-IDF 修复版本* 描述信息。
2024/01/19	V1.0	首次发布。