Security Advisory
安全公告

Title/标题	Security Advisory for WFA vulnerability 有关 WFA 漏洞的安全公告
Issue date/发布日期	2021-06-25
Advisory Number/公告编号	AR2021-003
Serial Number/编号	CVE-2020-24587 CVE-2020-24588 CVE-2020-26146 CVE-2020-26147 CVE-2020-24586
Version/版本	V1.0

Issue Summary

问题小结

Recently, the research paper “Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation” by Mathy Vanhoef disclosed a collection of security vulnerabilities that affect Wi-Fi devices. Three of these vulnerabilities are design flaws in the standard, while other nine are implementation vulnerabilities. More details about these vulnerabilities can be found here.

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。

The following vulnerabilities have been found to affect Espressif devices:

我们发现，乐鑫设备可能受到本次披露中以下漏洞的影响：

1) CVE-2020-24587: Mixed key attack (reassembling fragments encrypted under different keys).混合密钥攻击（重组在不同密钥下加密的片段）。

2) CVE-2020-24588: Aggregation attack (accepting non-SPP A-MSDU frames). 聚合攻击（接受 non-SPP A-MSDU 帧）。
3) CVE-2020-26146: Reassembling encrypted fragments with non-consecutive packet numbers. 重组非连续的加密片段。
4) CVE-2020-26147: Reassembling mixed encrypted/plaintext fragments. 重组混合加密/明文片段。
5) CVE-2020-24586: Fragment cache attack (not clearing fragments from memory when (re)connecting to a network). 分片缓存攻击（当[重新]连接到网络时，不从内存中清除片段）。

An attacker can use these vulnerabilities for the purpose of leaking information and exfiltration. To exploit these vulnerabilities, successful orchestration of injecting 802.11 packets, MITM attack and redirection to malicious server hosted by the attacker is required. Executing such combination in practice is difficult to achieve.
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。

Note that the attacks do not allow the attacker to bypass network layer protections such as TLS.
请注意，这些攻击无法绕过 TLS 等网络层安全特性。

Espressif thanks Dr Mathy Vanhoef for following a responsible disclosure process.
乐鑫感谢 Mathy Vanhoef 博士负责任地披露了此次问题。

Patched versions of ESP-IDF

ESP-IDF 修补版本

· Master (ef127ab9)
· Release v4.3.1 (46144f70)
· Release v4.2.2 (60ccb3fe)
· Release v4.1.2 (97c8be71)
· Release v4.0.4 (7504329e)
· Release v3.3.6 (b403b0db)

Patched versions of ESP8266 SDK

ESP8266 SDK 修补版本

- Master (08e225dd)
- Release v3.4 (967752e2)

Recommendations for Espressif Wi-Fi Devices

有关使用乐鑫 Wi-Fi 设备的建议

If your firmware application makes use of network transport layer security such as TLS, the immediate impact is low. This should also include use of HTTPS for connecting to any websites. Use of PMF(802.11w), WPA3 and EAP-TLS, if present, should further enhance security and prevent against MITM attacks. However, you should immediately update to the latest stable ESP-IDF or SDK bugfix release once it is available.

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。

If your firmware application does not use network transport layer security features such as TLS to protect important data or does not use latest Wi-Fi security protocols such as PMF/WPA3, you should consider urgently updating to a pre-release ESP-IDF or SDK version or updating to the latest stable release version.

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。

Audit all firmware applications to make sure any sensitive data is transferred using TLS or similar protocols and to verify that TLS is correctly configured.

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。

Audit all firmware applications to make sure that unknown websites are not navigated by any means and HTTPS is used to connect to the websites.

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。