安全公告
Security Advisory

标题/Title	Security Advisory concerning Wi-Fi authentication bypass 有关“绕过 Wi-Fi 验证漏洞”的安全公告
发布日期/Issue date	2020-7-23
公告编号/Advisory Number	AR2020-002
编号/Serial Number	CVE-2020-12638
版本/Version	V1.0

Issue Summary
小结

When an ESP32 or ESP8266 SoC is connected to an encrypted Wi-Fi access point, an attacker who injects a forged Wi-Fi beacon frame impersonating the access point can cause the SoC to switch to open authentication mode.
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。

The SoC will not be able to continue communicating with the encrypted access point for the duration of attack (provided attacker keeps sending forged beacon frames). During this period, the authentication mode of the SoC will toggle between open and encrypted. The attacker can then choose to send a forged Channel Switch Announcement, thereby switching the association to a different channel for the purpose of maintaining an open authentication connection to a different access point.
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。

The impact of this attack is that the SoC will transmit some Wi-Fi frames unencrypted. The SoC can also be made to associate with an attacker-controlled

open access point, allowing TCP/IP access by an attacker who does not have any access to the genuine Wi-Fi access point.
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。

The attack does not allow the attacker to bypass network-layer protections such as TLS. The attack does not allow the attacker to obtain any access to the genuine encrypted Wi-Fi access point.
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。

This issue was found and disclosed to Espressif by Lukas Bachschwell. Mr Bachschwell also registered CVE-2020-12638. Espressif thanks Mr Bachschwell for following a responsible disclosure process.
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。

Fixes
修复

ESP32

The issue is fixed in the ESP-IDF V3.2.4 release and will be fixed in the following upcoming ESP-IDF bugfix releases: V4.0.2, V3.3.3, V3.1.8 as well as V4.1 and newer versions.
这个问题已经在 ESP-IDF V3.2.4 版本中得到修复，并将在以下 ESP-IDF bug fix 版本：V4.0.2、V3.3.3、V3.2.5、V3.1.8，和 V4.1 及之后版本中得到修复。

Pre-release ESP-IDF branches containing the fix:
以下 IDF 分支均已经包含此次修复：

- master branch: commit 0dba9329
- release/v4.2 branch: commit ad5c4eb3
- release/v4.1 branch: commit b6e2163e
- release/v4.0 branch: commit 68b272f5
- release/v3.3 branch: commit 4891fcea
- release/v3.2 branch: commit a5c8cdd3
- release/v3.1 branch: commit a280fb32

For an explanation of ESP-IDF release branches and stable release versions, please refer to ESP-IDF documentation.
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

The issue is fixed in the following ESP8266 RTOS SDK branches:

以下 ESP8266 RTOS SDK 中均包含此次修复：

master branch: commit da3362ec

release/v3.3 branch: commit 9c72c21b

release/v3.2 branch: commit 3cbc3d87

release/v3.1 branch: commit 4b1ff5c3

release/v3.0 branch: commit 6ef5c2c2

release/v2.1 branch: commit db188200

The issue is fixed in the ESP8266 NON-OS SDK commit: be2f86d3.

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

ESP32-S2

There is not yet any stable ESP-IDF release supporting ESP32-S2. The release/v4.2 and master branches both have merged fixes for this issue (see above). The upcoming ESP-IDF V4.2 stable release (first to support ESP32-S2) will not be vulnerable to this issue.
目前，还没有任何支持 ESP32-S2 的稳定 ESP-IDF 版本。release/v4.2 和 master 分支都包括了对这个问题的修复。即将发布的 ESP-IDF V4.2 稳定版本（即首个支持 ESP32-S2 的稳定发布版本）将不会受到这个问题的影响。

Recommendations for Espressif Wi-Fi Devices
对使用乐鑫 Wi-Fi 设备者的建议

If your firmware application makes use of network transport layer security such as TLS, the immediate impact is low. 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。

If your firmware application does not use network transport layer security features such as TLS to protect important data, 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。

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. This is to protect against an attacker on the same network.
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。

Audit all firmware applications to make sure any network services served from the device will authenticate network clients before performing any trusted function. If the service receives credentials, a secure protocol such as TLS should be used to transfer them.
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。

Disclosure Timeline
披露时间线

30 May 2020: Issue report received.
2020 年 5 月 30 日，收到问题报告。

17 June 2020: Fix confirmed by reporter in ESP-IDF master branch.
2020 年 6 月 17 日，问题披露者已确认 ESP-IDF master 分支上的修复。

23 July 2020: Agreed public disclosure date.
2020 年 7 月 23 日：商定的公开披露日期。