Security Advisory

Title	Security Advisory Concerning Wi-Fi Authentication Bypass
Issue Date	2023/11/03
Advisory Number	AR2020-002
Serial Number	CVE-2020-12638
Version	V1.1

Issue Summary

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.

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.

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.

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.

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.

Fixes

ESP32

The issue is fixed in ESP-IDF v3.1.8, v3.2.4, v3.3.3, v4.0.2, v4.1, v4.2 and later versions.

ESP-IDF branches containing the fix:

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.

ESP8266

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

master branch: commit da3362ec
release/v3.4 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.

ESP32-S2

The release/v4.2 and master branches both have merged fixes for this issue (see above). ESP-IDF v4.2 stable release, which is the first ESP-IDF version that supports ESP32-S2, and later versions are not affected by this issue.

Recommendations for Espressif Wi-Fi Devices

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.

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.

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.

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.

Revision History

Date	Version	Release notes
2023/11/03	V1.1	Update the fix information in Part Fixes.
2020/07/23	V1.0	Initial release.