ESPRESSIF

Security Advisory

Title	Security Advisory for WFA vulnerability
Issue Date	2023/08/25
Advisory Number	AR2021-003
Serial Number	CVE-2020-24586 CVE-2020-24587 CVE-2020-24588 CVE-2020-26146 CVE-2020-26147
Version	V1.1

Issue Summary

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.

The following vulnerabilities have been found to affect Espressif devices:

- Wi-Fi design flaws：
  1) CVE-2020-24586: Fragment cache attack (not clearing fragments from memory when (re)connecting to a network).
  2) CVE-2020-24587: Mixed key attack (reassembling fragments encrypted under different keys).
  3) CVE-2020-24588: Aggregation attack (accepting non-SPP A-MSDU frames).

- Wi-Fi implementation vulnerabilities:
  1) CVE-2020-26146: Reassembling encrypted fragments with non-consecutive packet numbers.
  2) CVE-2020-26147: Reassembling mixed encrypted/plaintext fragments.

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.

Note that the attacks do not allow the attacker to bypass network layer protections such as TLS.

Espressif thanks Dr Mathy Vanhoef for following a responsible disclosure process.

Patched Versions of ESP-IDF

ESP-IDF Branch	Fixed ESP-IDF Version	Commit ID with the Fix
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

Patched Versions of ESP8266 SDK

ESP8266 SDK Branch	Commit ID with the Fix
master	08e225dd
release/v3.4	967752e2

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. 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.

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.

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.

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.

Revision History

Date	Version	Release notes
2023/08/25	V1.1	1. Separate AR2021-003 as EN & CN version. 2. Update information in chapter *Issue Summary*, *Patched Versions of ESP-IDF* and *Patched Versions of ESP8266 SDK*.
2021/06/25	V1.0	Initial release.