Security Advisory

Title	Security Advisory for WLAN FragAttacks
Issue Date	2024/05/10
Advisory Number	AR2023-008
Serial Number	CVE-2020-26142
Version	V1.1

Issue Summary

Fragattacks were a set of CVEs that were made public in May 2021. These were MITM attacks on Wi-Fi devices based on WLAN Fragmentation and/or AMPDU usage.

The following Wi-Fi implementation vulnerability was found on Espressif device:

A vulnerable Espressif WLAN device processes every single fragmented AMPDU frame as an independent and a full frame and the same could get passed till the application layer. It is an attack case where-in an MITM attacker can control the WLAN device to load a malicious URL, just by managing to spoof one of the multiple fragments.

Impact Analysis

Vulnerability impacts when the use case does not involve any transport layer security, e.g. loading URLs using HTTP protocol.

However, the attacks cannot bypass transport layer security on the network layer, e.g. loading URLs using HTTPS protocol.

Affected Espressif Products Series:

ESP8266, ESP32, ESP32-S2, ESP32-C2, ESP32-S3, ESP32-C3, ESP32-C6.

Affected Versions of ESP8266 RTOS SDK:

ESP8266 RTOS SDK Branch	Affected Commit ID	Affected ESP8266 RTOS SDK Version
master	Any commit before 816bf9bc	/
release/v3.4	Any commit before d47d0f4d	release/v3.4

Affected Versions of ESP-IDF:

ESP-IDF Branch	Affected Commit ID	Affected ESP-IDF Version
master	Any commit before 7ae8e1c4	/
release/v5.2	Any commit before 89dcaf4a	v5.2
release/v5.1	Any commit before 70f1bd58	v5.1 - v5.1.2
release/v5.0	Any commit before 5402e14c	v5.0 - v5.0.4
release/v4.4	Any commit before 629c3b4d	v4.4 - v4.4.6
release/v4.3	Any commit before 37b1fc9d	v4.3 - v4.3.6

Mitigation

Patched Versions of ESP8266 RTOS SDK:

ESP8266 RTOS SDK Branch	Fixed Commit ID	Fixed ESP8266 RTOS SDK Version
master	816bf9bc	/
release/v3.4	d47d0f4d	release/v3.4

Patched Versions of ESP-IDF:

ESP-IDF Branch	Fixed Commit ID	Fixed ESP-IDF Version
master	7ae8e1c4	/
release/v5.2	89dcaf4a	v5.2.1

release/v5.1	70f1bd58	v5.1.3
release/v5.0	5402e14c	v5.0.5
release/v4.4	629c3b4d	v4.4.7
release/v4.3	37b1fc9d	v4.3.7

Recommendations for Application Developers

While using Espressif WLAN products in your deployments, for data security and protection against attacks our recommendations are as follows:

1. If the network layer TLS is disabled, we recommend you to enable it and move to the latest stable ESP-IDF releases.

2. If the application or the WLAN network has PMF or WPA3 disabled, we recommend enabling them for added security at the data link layer.

3. Make sure HTTPS is used to connect to all websites, without an option to bypass HTTPS.

Revision History

Date	Version	Release notes
2024/05/10	V1.1	Updated *Fixed ESP-IDF Version* description.
2024/01/19	V1.0	Initial release.