Security Advisory

Title	Security Advisory for PEAP Phase-2 authentication
Issue Date	2024/06/03
Advisory Number	AR2024-003
Serial Number	CVE-2023-52160
Version	V1.0

Issue Summary

PEAP is a Protected Extensible Authentication protocol that extends EAP by encapsulating EAP connection within TLS tunnel.

This was a common issue in supplicant and the details are as follows:

In PEAP, the client's behavior permitted servers to bypass Phase 2 authentication, assuming that the server was authenticated during Phase 1 via TLS server certificate validation. The specification for PEAP lacked clarity on this matter, resulting in greater flexibility than other methods like TTLS, FAST and TEAP. This is advantageous in a few cases but becomes problematic in some scenarios where PEAP is misconfigured.

One common misconfiguration occurs when the server's trust root (ca-cert) which is essential for verifying authenticity in TLS handshake is not properly configured. Additionally, users sometimes have the option to bypass or ignore the validation step easily.

This could potentially expose the network to security threats, as authentication might not be as robust as intended.

Impact Analysis

This vulnerability can impact the users that use Wi-Fi Enterprise network with PEAP in case of attack where an attacker can deceive by setting up fraudulent clones of

the Enterprise network and luring victims to connect and subsequently intercept their traffic.

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 898bf9e4	NA
release/v3.4	Any commit before 0cac4f8cf	release/v3.4

ESP-IDF Affected Versions:

ESP-IDF Branch	Affected Commit IDs	Affected ESP-IDF Versions
master	Any commit before 59a62f2af	NA
release/v5.2	Any commit before b761052e	Any version before v5.2.2
release/v5.1	Any commit before 6f9cc06b	Any version before v5.1.4
release/v5.0	Any commit before 34121bde	Any version before v5.0.7
release/v4.4	Any commit before 4db2ef0f3	Any version before v4.4.8

Mitigation

Patched Versions of ESP8266 RTOS SDK:

ESP8266 RTOS SDK Branch	Fixed Commit ID	Fixed ESP8266 RTOS SDK Version
master	898bf9e4	NA
release/v3.4	0cac4f8cf	release/v3.4

ESP-IDF Patched Versions:

ESP-IDF Branch	Fixed Commit ID	Fixed ESP-IDF Version
master	59a62f2af	NA
release/v5.2	b761052e	Expected in v5.2.2

release/v5.1	6f9cc06b	v5.1.4
release/v5.0	34121bde	Expected in v5.0.7
release/v4.4	4db2ef0f3	Expected in v4.4.8

Recommendations for Application Developers

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

- Move to the latest stable ESP-IDF release as it contains changes where the “phase2_auth” option is by default set to 1 meaning phase2_authentication will be required for initial connection, in the case when client certificate (private key/client_cert) is not used and TLS session resumption was not used.

- Change the default PEAP client behavior to mandate successful completion of Phase 2 authentication, except in cases of TLS session resumption or when the client certificate is configured.