安全公告

标题	PEAP 第二阶段认证安全公告
发布日期	2024/06/03
公告编号	AR2024-003
编号	CVE-2023-52160
版本	V1.0

问题小结

PEAP 是一种受保护的可扩展认证协议，通过在 TLS 通道内封装 EAP 连接来扩展 EAP。

然而，目前存在如下客户端问题：

在 PEAP 中，假设服务器在第一阶段通过 TLS 服务器证书验证进行了认证，客户端允许服务器绕过第二阶段认证。PEAP 规范在这一问题上没有明确规定，因此比 TTLS、FAST 和 TEAP 等其他方法更具灵活性。在某些情况下灵活性能够带来便利，但在 PEAP 配置错误时可能会产生问题。

常见的配置错误之一是服务器的根证书 (ca-cert) 未正确配置，这对于 TLS 握手中验证的真实性至关重要。此外，用户有时可以轻松地绕过或忽略验证步骤。

上述问题可能造成网络安全威胁，导致认证不如预期可靠。

影响分析

这种漏洞可能会影响使用 PEAP Wi-Fi 企业网络的用户。攻击者可以通过克隆企业网络诱使受害者连接网络，然后截取其流量。

影响产品系列

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

ESP8266 RTOS SDK 问题版本

ESP8266 RTOS SDK 分支	问题 Commit ID	ESP8266 RTOS SDK 问题版本
master	898bf9e4 之前所有 commit	NA
release/v3.4	0cac4f8cf 之前所有 commit	release/v3.4

ESP-IDF 问题版本

ESP-IDF 分支	问题 Commit ID	ESP-IDF 问题版本
master	59a62f2af 之前所有 commit	NA
release/v5.2	b761052e 之前所有 commit	v5.2.2 之前所有版本
release/v5.1	6f9cc06b 之前所有 commit	v5.1.4 之前所有版本
release/v5.0	34121bde 之前所有 commit	v5.0.7 之前所有版本
release/v4.4	4db2ef0f3 之前所有 commit	v4.4.8 之前所有版本

修复措施

ESP8266 RTOS SDK 修复版本

ESP8266 RTOS SDK 分支	修复 Commit ID	ESP8266 RTOS SDK 修复版本
master	898bf9e4	NA
release/v3.4	0cac4f8cf	release/v3.4

ESP-IDF 修复版本

ESP-IDF 分支	修复 Commit ID	ESP-IDF 修复版本
master	59a62f2af	NA
release/v5.2	b761052e	预计在 v5.2.2 中修复
release/v5.1	6f9cc06b	v5.1.4
release/v5.0	34121bde	预计在 v5.0.7 中修复
release/v4.4	4db2ef0f3	预计在 v4.4.8 中修复

给应用程序开发人员的建议

在部署乐鑫 WLAN 产品时，为了保护数据安全，我们建议：

- 迁移到最新的稳定 ESP-IDF 版本。最新版本中，phase2_auth 选项默认为 1，表示在未使用客户端证书（私钥/client_cert）以及 TLS 会话恢复的情况下，初始连接需要第二阶段认证。

- 将默认的 PEAP 客户端行为更改为要求完成第二阶段认证，除非使用了 TLS 会话恢复或客户端证书。