Bug 公告

标题	ESP-IDF 中 WPA3-SAE H2E 配置问题的 OTA 公告
发布日期	2026/04/29
公告编号	AR2026-003
编号	NA
版本	V1.0

问题小结

SAE（对等实体同时认证）是一种基于密码的安全认证与密钥协商协议，用于 WPA3 个人版 Wi-Fi 连接。SAE 采用了哈希到元素 (H2E) 等机制以增强安全性。本公告涉及乐鑫 ESP-IDF 框架中，在无线升级过程中处理 SAE 连接的 H2E 参数（*sae_pwe_h2e* 和 *sae_h2e_identifier*）时相关的多个软件问题。在特定条件下，这些问题会导致 OTA 升级后 station 模式或 SoftAP 模式的 Wi-Fi 连接失败，其主要原因在于 Wi-Fi 配置结构中这些值的错误获取、设置或解析。

问题详情

问题 1：OTA 升级后 station 模式 SAE 连接失败
当使用 *esp_wifi_get_config* 从 *wifi_sta_config_t* 中获取 *sae_pwe_h2e* 值，再通过 *esp_wifi_set_config* 将其写回时，获取到的值不正确，导致 OTA 后连接失败。

问题 2：OTA 升级后 SoftAP 模式 SAE 连接失败
与问题 1 类似，使用 *esp_wifi_get_config* 从 *wifi_ap_config_t* 中获取 *sae_pwe_h2e* 值，再通过 *esp_wifi_set_config* 将其写回时，获取到的值不正确，导致 OTA 后 SoftAP 连接失败。

问题 3：若 sae_pwe_h2e 未设为 “Hunt and Peck”，SAE 连接失败
OTA 升级后，*sae_h2e_identifier* 的默认 NVS 值被设置为 0xFF*32。当 OTA 后调用 *esp_wifi_set_config()* 时，该函数要么显式设置一个有效的 *sae_h2e_identifier* 值，要么在未提供用户定义值时将其重置为 0。若 OTA 后未使用 *esp_wifi_set_config()* 修改默认的 NVS 值，则值 0xFF*32 会被视为有效配置，从而导致 OTA 后 SAE 连接失败。

问题 4：*sae_pwe_h2e* 的默认 NVS 值导致互操作性问题

sae_pwe_h2e 的默认 NVS 值为 0，在内部映射为 Hunt-and-Peck 模式。此值会以下列方式限制安全功能：

问题 4.1 Station 模式
该 sae_pwe_h2e 值强制设备仅连接支持 Hunt-and-Peck 的 AP。仅支持 H2E 的 AP 会被忽略，导致与这些 AP 的连接失败。

问题 4.2 SoftAP 模式
SoftAP 仅以 Hunt-and-Peck 模式启动，这会导致仅需要 H2E 模式的客户端无法连接。

影响分析

这些问题会影响那些在个人网络中依赖使用 WPA3-SAE 来实现安全 Wi-Fi 连接的用户。OTA 升级后，设备可能无法重新连接网络，从而导致服务中断、停机或需要手动干预（例如恢复出厂设置）。在关键的物联网部署中，这可能会降低整体可靠性。尽管不涉及直接的安全漏洞（如未经授权的访问），但如果用户因反复连接失败而选择降级到安全性较低的 Wi-Fi 协议，则可能间接增加风险。

如果应用程序启用了 ESP-IDF OTA 应用程序回滚功能，并在新固件启动后设置了一个有效的检查点（例如，成功连接 Wi-Fi 或成功接入 OTA 服务器），那么即使某次错误的 OTA 升级破坏了 Wi-Fi 功能，系统仍然可以回滚到上一个已知正常运行的应用程序。

对于问题 1 和 2，若用户在 OTA 升级后，使用 esp_wifi_get_config 和 esp_wifi_set_config API 修改了 Wi-Fi 存储 NVS 中的 sae_h2e_pwe 值，则回滚操作将失败。此外，如果在受影响版本上对 sae_h2e_pwe 调用 esp_wifi_get_config 和 esp_wifi_set_config，会将错误的值写入 NVS，即使随后升级到已修复版本，也可能导致连接问题。为了规避此风险，请在烧录了修正后的固件版本后，使用 esp_wifi_set_config 执行一次显式的 NVS 重写操作。

影响产品系列

问题 1 影响 ESP32、ESP32-S2、ESP32-C2、ESP32-S3、ESP32-C3 和 ESP32-C6。

问题 2 影响 ESP32、ESP32-S2、ESP32-C2、ESP32-S3、ESP32-C3 和 ESP32-C6。

问题 3 影响 ESP32、ESP32-S2、ESP32-C2、ESP32-S3、ESP32-C3、ESP32-C6、ESP32-C5 和 ESP32-C61。

问题 4.1 影响 ESP32、ESP32-S2、ESP32-C2、ESP32-S3、ESP32-C3、ESP32-C6、ESP32-C5 和 ESP32-C61。

问题 4.2 影响 ESP32、ESP32-S2、ESP32-C2、ESP32-S3、ESP32-C3、ESP32-C6、ESP32-C5 和 ESP32-C61。

影响 ESP-IDF 版本

问题	触发条件与 OTA 路径	影响 Commit ID	影响 ESP-IDF 版本
问题 1	station 模式下，在 OTA 过程中使用 *esp_wifi_get_config* / *esp_wifi_set_config* 错误处理 *sae_pwe_h2e* 参数	v5.1: 0b921fda v5.0.2: 7cf3f99b v4.4.5: b7ddd82a	v5.1 v5.0.2~v5.0.3 v4.4.5
问题 2	SoftAP 模式下，在 OTA 过程中使用 *esp_wifi_get_config* / *esp_wifi_set_config* 错误处理 *sae_pwe_h2e* 参数	v5.1: 146a5c4d	v5.1
问题 3	默认 NVS 值 (0xff+32) 被错误地视为有效连接配置	v5.1: a3b5472d	v5.5~v5.5.1 v5.4~v5.4.2 v5.3~v5.3.4 v5.2~v5.2.5 v5.1~v5.1.6
问题 4.1	*sae_pwe_h2e* 的默认 NVS 值导致 station 模式互操作性问题	v5.1: 0b921fda v5.0.2: 7cf3f99b v4.4.5: b7ddd82a v4.3.6: 637f491e	v5.5~v5.5.2 v5.4~v5.4.3 v5.3~v5.3.4 v5.2~v5.2.6 v5.1~v5.1.6 v5.0.2~v5.0.9 v4.4.5~v4.4.8 v4.3.6~v4.3.7
问题 4.2	*sae_pwe_h2e* 的默认 NVS 值导致 SoftAP 模式互操作性问题	v5.1: 146a5c4d	v5.5~v5.5.2 v5.4~v5.4.3 v5.3~v5.3.4 v5.2~v5.2.6 v5.1~v5.1.6

应对方法

ESP-IDF 修复版本

问题	修复 Commit ID	ESP-IDF 修复版本
问题 1	v5.2: 29a3f865 v5.1: a09a5030 v5.0: b4b43066 v4.4: 3b570fd9	v5.2 v5.1.1+ v5.0.4+ v4.4.6+

问题 2	v5.2: 29a3f865 v5.1: a09a5030	v5.2+ v5.1.1+
问题 3	v6.0: 44736c8b v5.5: 5e481987 v5.4: 8574a0a6 v5.3: b16a2250 v5.2: b6f95aa2 v5.1: dfe9d705	v6.0+ v5.5.2+ v5.4.3+ v5.3.5+ v5.2.6+ v5.1.7+
问题 4.1	v6.0: 3f577994 v5.5: a3927641 v5.4: 9f2841dd v5.3: b9f3173f v5.2: 256200fb v5.1: ac7dabaf	v6.0+ v5.5.3+ v5.4.4+ v5.3.5+ v5.2.7+ v5.1.7+
问题 4.2	v6.0: 3f577994 v5.5: a3927641 v5.4: 9f2841dd v5.3: b9f3173f v5.2: 256200fb v5.1: ac7dabaf	v6.0+ v5.5.3+ v5.4.4+ v5.3.5+ v5.2.7+ v5.1.7+

变通方法

在所有问题得到彻底修复之前，建议采取以下规避措施：

问题 1：
- 使用 *esp_wifi_set_config* 时，不要基于 *esp_wifi_get_config* 返回的值来设置 *sae_pwe_h2e*。
- 避免 OTA 升级至 v4.4.5、v5.0.2、v5.0.3、v5.1 版本。

问题 2：
- 使用 *esp_wifi_set_config* 时，不要基于 *esp_wifi_get_config* 返回的值来设置 *sae_pwe_h2e*。
- 避免 OTA 升级至 v5.1 版本。

问题 3：
- 使用 *esp_wifi_set_config* 显式设置 *sae_h2e_identifier*。
- 升级至 v5.1 或更高版本时，也不要通过 *esp_wifi_get_config* 获取的值来设置 *sae_h2e_identifier*。
- 建议在修复版本发布后，升级到更新的 ESP-IDF 版本。

问题 4.1 和 4.2：
- 使用 *esp_wifi_set_config* 将 *sae_pwe_h2e* 显式设置为 *WPA3_SAE_PWE_BOTH*。
- 建议在修复版本发布后，升级到更新的 ESP-IDF 版本。

给应用程序开发者的建议

我们强烈建议开发者在修复版本发布后，尽快迁移至最新的稳定版 ESP-IDF。在过渡期间，请遵循上述变通方法，以防止 OTA 后出现 Wi-Fi 重连问题。请显式管理 *sae_pwe_h2e* 和 *sae_h2e_identifier* 的值，而非依赖 NVS 或 *esp_wifi_get_config* 中的默认值。

在已修复的 ESP-IDF 版本中，H2E 密码标识符的校验逻辑已得到改进。现在，无论是空终止字符串（长度小于 SAE_H2E_IDENTIFIER_LEN）还是非空终止字符串（长度等于 SAE_H2E_IDENTIFIER_LEN），均能被正确接受。但整个 SAE_H2E_IDENTIFIER_LEN 长度范围内全部填充为 0xFF 的值，不再被视为有效的标识符。