Bug Advisory

Title	OTA Bug Advisory for WPA3-SAE H2E Configuration Issues in ESP-IDF
Issue Date	2026/04/29
Advisory Number	AR2026-003
Serial Number	NA
Version	V1.0

Issue Summary

SAE (Simultaneous Authentication of Equals) is a secure, password-based authentication and key establishment protocol used in WPA3-Personal mode for Wi-Fi connections. SAE incorporates mechanisms such as Hash-to-Element (H2E) to enhance security. This advisory addresses multiple software issues in Espressif's ESP-IDF framework related to the handling of H2E parameters (*sae_pwe_h2e* and *sae_h2e_identifier*) in SAE connections during Over-The-Air (OTA) updates. Under specific conditions, these issues may cause Wi-Fi connection failures in both Station (STA) or SoftAP modes due to incorrect retrieval, configuration, or interpretation of these parameters.

Issue details

Issue 1: SAE Connection Failure in Station Mode After OTA
Retrieving *sae_pwe_h2e* value from *wifi_sta_config_t* using *esp_wifi_get_config* and then restoring it via *esp_wifi_set_config* may result in an incorrect value, leading to connection failures after OTA.

Issue 2: SAE Connection Failure in SoftAP Mode After OTA
Similar to issue 1, retrieving *sae_pwe_h2e* value from *wifi_ap_config_t* using *esp_wifi_get_config* and restoring it via *esp_wifi_set_config* may produce an incorrect value, causing SoftAP connection failures after OTA.

Issue 3: SAE Connection Failure When *sae_pwe_h2e* Is Not "Hunt and Peck"
After an OTA update, the default NVS value of *sae_h2e_identifier* is set to 0xFF*32. When *esp_wifi_set_config()* is invoked, it may either set a valid *sae_h2e_identifier* value or reset it to 0 if no user-defined value is provided.

If *esp_wifi_set_config()* is not used to modify the default NVS value post OTA, the value 0xFF*32 is treated as a valid configuration, which leads to SAE connection failures after OTA.

Issue 4: Default NVS Value of *sae_pwe_h2e* Causes Interoperability Issues
The default NVS value of *sae_pwe_h2e* is set to 0, which maps internally to **Hunt-and-Peck** mode. This value can limit interoperability as follows.

Issue 4.1: Station Mode
This *sae_pwe_h2e* value forces the device to connect **only** to APs that support Hunt-and-Peck. APs that support **H2E only** are ignored, leading to connection failures with those APs.

Issue 4.2 : SoftAP Mode
The SoftAP operates in **Hunt-and-Peck mode only**, which prevents clients that require H2E only from connecting.

Impact Analysis

These issues can impact users relying on WPA3-SAE for secure Wi-Fi connections in personal networks. After an OTA update, devices may fail to reconnect to networks, leading to service disruptions, downtime, or the need for manual intervention (e.g., factory resets). In critical IoT deployments, this can reduce overall reliability. Although no direct security exploit (e.g., unauthorized access) is involved, repeated connection failures could indirectly increase risk if users choose to downgrade to less secure Wi-Fi protocols.

If application enables the ESP-IDF OTA app rollback feature and uses a valid checkpoint after the new firmware boots (for example, successful Wi-Fi connection or successful contact with your OTA server), a bad OTA that breaks Wi-Fi can still be rolled back to the previous known-good application.

Rollback will fail for Issues 1 & 2 provided customer alters WIFI Storage NVS values after OTA using esp_wifi_get_config and esp_wifi_set_config APIs for sae_h2e_pwe value. Additionally, if esp_wifi_get_config and esp_wifi_set_config is called on affected version for sae_h2e_pwe, writing incorrect values in NVS, can cause connection issues even after upgrading to fixed releases. To mitigate this, perform an explicit NVS rewrite using esp_wifi_set_config after flashing a corrected firmware version.

Affected Product Series:

Issue 1: ESP32, ESP32-S2, ESP32-C2, ESP32-S3, ESP32-C3, ESP32-C6

Issue 2: ESP32, ESP32-S2, ESP32-C2, ESP32-S3, ESP32-C3, ESP32-C6

Issue 3: ESP32, ESP32-S2, ESP32-C2, ESP32-S3, ESP32-C3, ESP32-C6, ESP32-C5, ESP32-C61

Issue 4.1: ESP32, ESP32-S2, ESP32-C2, ESP32-S3, ESP32-C3, ESP32-C6, ESP32-C5, ESP32-C61

Issue 4.2: ESP32, ESP32-S2, ESP32-C2, ESP32-S3, ESP32-C3, ESP32-C6, ESP32-C5, ESP32-C61

ESP-IDF Affected Versions:

Issue	Trigger Condition/OTA Path	Issue Introducing Commits	Affected Versions
Issue 1	OTA with *esp_wifi_get_config* / *esp_wifi_set_config* handling *sae_pwe_h2e* incorrectly for station	v5.1: 0b921fda v5.0.2: 7cf3f99b v4.4.5: b7ddd82a	v5.1 v5.0.2~v5.0.3 v4.4.5
Issue 2	OTA with *esp_wifi_get_config* / *esp_wifi_set_config* handling *sae_pwe_h2e* incorrectly for SoftAP	v5.1: 146a5c4d	v5.1
Issue 3	Default NVS value (0xff+32) incorrectly treated as valid for connection	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
Issue 4.1	Default NVS value for *sae_pwe_h2e* causes station interoperability issues	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
Issue 4.2	Default NVS value for *sae_pwe_h2e* causes SoftAP interoperability issues	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

Mitigation

ESP-IDF Patched Versions:

Issue	Fixed Commits	Fixed ESP-IDF Versions
Issue 1	v5.2: 29a3f865 v5.1: a09a5030 v5.0: b4b43066 v4.4: 3b570fd9	v5.2 v5.1.1+ v5.0.4+ v4.4.6+

Issue 2	v5.2: 29a3f865 v5.1: a09a5030	v5.2+ v5.1.1+
Issue 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+
Issue 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+
Issue 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+

Workaround

Until all issues are fully patched, the following workarounds are recommended:

Issue 1 (Station failure)

- When using *esp_wifi_set_config*, do not set *sae_pwe_h2e* based on *esp_wifi_get_config*.
- Avoid OTA upgrades to v4.4.5, v5.0.2, v5.0.3, v5.1.

Issue 2 (SoftAP failure)

- When using *esp_wifi_set_config*, do not set *sae_pwe_h2e* based on *esp_wifi_get_config*.
- Avoid OTA upgrades to v5.1.

Issue 3 (NVS handling failure)

- Use *esp_wifi_set_config* to explicitly set *sae_h2e_identifier*.
- When upgrading to v5.1 or above, also avoid setting *sae_h2e_identifier* from *esp_wifi_get_config*.
- Prefer to upgrade to newer ESP-IDF versions once a fix is released.

Issue 4.1 and Issue 4.2 (Default NVS *sae_pwe_h2e*)

- Use *esp_wifi_set_config* to explicitly set *sae_pwe_h2e* to WPA3_SAE_PWE_BOTH.
- Prefer to upgrade to newer ESP-IDF versions once a fix is released.

Recommendations for Application Developers

While Developers are strongly advised to move to the latest stable ESP-IDF releases once fixes are integrated. For the interim, follow the workarounds outlined above to prevent Wi-Fi reconnection issues post-OTA. Explicitly manage *sae_pwe_h2e* and *sae_h2e_identifier* values rather than relying on defaults from NVS or *esp_wifi_get_config*.

In the fixed ESP-IDF versions, the H2E password identifier validation has been improved. Both null-terminated strings (length < SAE_H2E_IDENTIFIER_LEN) and non-null-terminated strings (length = SAE_H2E_IDENTIFIER_LEN) are accepted. However, a value filled with 0xFF for the entire SAE_H2E_IDENTIFIER_LEN length is no longer considered a valid identifier.