Advisory TFMV-3

Title	abort() function may not take effect in TF-M Crypto multi-part MAC/hashing/cipher operations
CVE ID	CVE-2021-32032
Date	April 29, 2021
Versions	Affected all versions up to and including TF-M v1.3.0
Configurations	All configurations
Impact	It can cause memory leakage in TF-M Crypto service, eventually making TF-M Crypto service unavailable and impacting other services relied on it.
Fix Version	SHA for trusted-firmware-m Git repository will be provided after patches merge
Credit	Chongqing Lei, Southeast University Zhen Ling, Associate Professor, Southeast University Xinwen Fu, Professor, University of Massachusetts Lowell

Background

PSA multi-part crypto operation sequence

PSA Crypto API specification defines a common sequence for all multi-part crypto operations. The sequence can be simplified to the following steps:

- `setup()`
  Set up the multi-part operation.
- `update()`
  Add data/configurations into the multi-part operation.
- `finish()`
  Complete the multi-part operation.

PSA Crypto API specification requests that the corresponding `abort()` function shall be called when `update()` or `finish()` function fails. The `abort()` function aborts the ongoing multi-part operation and cleans up the operation context.

TF-M multi-part crypto operation functions eventually call the underlying crypto library (Mbed TLS by default) to perform those steps, including `abort()` step.

PSA multi-part crypto operation objects

PSA Crypto API specification defines an operation object for each type of multi-part crypto operations. For example, `psa_mac_operation_t` for multi-part MAC operations and `psa_hash_operation_t` for multi-part hashing operations.

TF-M Crypto service relies on the underlying crypto library (Mbed TLS by default) to implement those objects. The structures of those objects are crypto library specific and hidden to TF-M.

The underlying crypto library usually stores and manages the context of ongoing multi-part crypto operations in the corresponding PSA operation object. For example, Mbed TLS stores multi-part hashing operation context in its `psa_hash_operation_t` implementation. The context is cleaned up in crypto library `abort()` function when the client calls `abort()` to handle a previous error. The clean-up execution can include zeroing the memory area and freeing allocated memory.

TF-M multi-part crypto operation objects

TF-M Crypto service defines a dedicated operation structure `tfm_crypto_operation_s` to wrap PSA multi-part crypto operation object and maintains its own status, as shown in the figure below.

```
struct tfm_crypto_operation_s {

    ……

    union {
        psa_cipher_operation_t cipher;    /*!< Cipher operation context */

        psa_mac_operation_t mac;          /*!< MAC operation context */

        psa_hash_operation_t hash;        /*!< Hash operation context */

        psa_key_derivation_operation_t key_deriv; /*!< Key derivation operation context */

    } operation;

};
```

TF-M Crypto service assigns a `tfm_crypto_operation_s` object for each multi-part crypto operation sequence during `setup()` step. The `tfm_crypto_operation_s` object content will be cleaned after the sequence completes or fails.

Impact

During multi-part hashing/MAC/cipher operations, if the underlying crypto library function returns an error code, TF-M `update()` and `finish()` functions will immediately clean up the structure `tfm_crypto_operation_s` content and exit.

When `tfm_crypto_operation_s` content is cleaned in TF-M `update()` and `finish()` functions, the content in PSA multi-part crypto operation object inside `tfm_crypto_operation_s` is also cleaned. If the underlying crypto library stores operation context in the PSA operation object, the operation context is lost before clients call `abort()` to handle the error.

Therefore, the underlying crypto library `abort()` function can be unable to perform normal abort operation if it cannot fetch the context or its content. In other words, the underlying crypto library `abort()` may not work normally or take effect.

The actual consequences depend on the implementation of the multi-part operations in the underlying crypto library.

In theory when the case analyzed above occurs:

- If the underlying crypto library dynamically allocates some memory regions during multi-part operation and stores those memory region pointers in the PSA multi-part operation object, the underlying crypto library will be unable to locate and free those allocated memory regions in `abort()`. It will cause memory leakage in TF-M Crypto service. It may further make TF-M Crypto service unavailable and affect other services relying on TF-M Crypto service.
- The underlying crypto library `abort()` may still consider the field values in the context as valid. `abort()` may perform unexpected behaviors or access invalid memory regions. It may trigger further faults and block TF-M Crypto service or even the whole system.

Impacted PSA Crypto API functions

The following PSA multi-part crypto operation functions are impacted:

- Multi-part hashing operations
  - `psa_hash_update()`
  - `psa_hash_finish()`
  - `psa_hash_verify()`
  - `psa_hash_clone()`
- Multi-part MAC operations
  - `psa_mac_update()`
  - `psa_mac_sign_finish()`
  - `psa_mac_verify_finish()`
- Multi-part cipher operations
  - `psa_cipher_generate_iv()`
  - `psa_cipher_set_iv()`
  - `psa_cipher_update()`
  - `psa_cipher_finish()`

Justifications on unaffected multi-part operations

TF-M multi-part AEAD operations and multi-part key derivation operations are not impacted by this issue.

TF-M Crypto service has not implemented multi-part AEAD operations. TF-M multi-part AEAD functions directly return an error of unsupported operations.

In TF-M key derivation implementation, the `psa_key_derivation_operation_t` object is only cleaned in the `abort()` function after the underlying crypto library completes abort.

Mitigation

The clean-up operation shall be removed from error handling routines in the following TF-M Crypto functions:

- Multi-part hashing operations
  - `tfm_crypto_hash_update()`
  - `tfm_crypto_hash_finish()`
  - `tfm_crypto_hash_verify()`
  - `tfm_crypto_hash_clone()`
- Multi-part MAC operations
  - `tfm_crypto_mac_update()`
  - `tfm_crypto_mac_sign_finish()`
  - `tfm_crypto_mac_verify_finish()`
- Multi-part cipher operations
  - `tfm_crypto_cipher_generate_iv()`
  - `tfm_crypto_cipher_set_iv()`
  - `tfm_crypto_cipher_update()`
  - `tfm_crypto_cipher_finish()`

Please note that this mitigation assumes that client follows the sequence specified in PSA Crypto API specification to call `abort()` when an error occurs during multi-part crypto operations.