PSA random generator cloning (CVE-2026-25835)

Title	PSA random generator cloning
CVE	CVE-2026-25835
Date	31 March 2026
Affects	all versions of Mbed TLS from 2.18.0 to 3.6.5; all versions of Mbed Crypto; TF-PSA-Crypto
Not affected	Mbed TLS 3.6.6 and later 3.6 versions; Mbed TLS 4.1.0 and later; TF-PSA-Crypto 1.1.0 and
Impact	Insufficient randomness
Severity	HIGH
Credits	internal

Vulnerability

Some applications and systems are *cloned*: the application state is copied, so there are multiple instances of the same application that initially have the same state. Common cases where this happens include:

- the `fork()` system call on Unix-like system;
- cloning of virtual machines;
- hibernation images that can be resumed multiple times.

When the application includes a random generator, cloning the random generator is insecure: all clones have the same state, and therefore, in most configurations, they will at least initially generate the same random numbers. It is therefore necessary to reseed the random generator after cloning, so that each instance ends up with an independent random generator state.

The PSA subsystem in TF-PSA-Crypto and Mbed TLS uses an internal random generator. Before Mbed TLS 3.6.6 and TF-PSA-Crypto 1.1.0, there is no interface to force a reseed of the PSA random generator, which makes it difficult to protect it against cloning. In addition, the library documentation does not explain how to protect random generators in legacy APIs against cloning.

Since TF-PSA-Crypto 1.0.0 and Mbed TLS 4.0.0, all random generation uses the random generator provided by the PSA subsystem. In previous versions, by default, the PSA subsystem is only used for PSA API calls and parts of TLS 1.3. When `MBEDTLS_USE_PSA_CRYPTO` is enabled, the PSA random generator is also used in parts of the PK, X.509 and TLS subsystems.

Impact

If the state of a random generator is cloned, both instances will produce the same output until the random generator reseeds. This can be very bad for security since both instances will produce the same keys, the same nonces, etc. An adversary could even interact with one instance to obtain random generator outputs that are public (e.g. a protocol nonce), and use that knowledge to attack the other instance (e.g. a victim's session key)..

Affected versions

All versions of Mbed TLS from 2.18.0 to 3.6.5, all versions of Mbed Crypto, Mbed TLS 4.0.0, and TF-PSA-Crypto 1.0.0 are affected.

In addition, all versions of the library are affected if the application is part of a cloned system image and does not take appropriate precautions as discussed in the "Resolution" section below.

Work-around

Applications are not affected if all of the following conditions are met:

- the library version is Mbed TLS 3.6.x or below;
- the compile-time option `MBEDTLS_USE_PSA_CRYPTO` is not enabled;
- the application does not call `psa_xxx()` APIs;
- the application does not use TLS 1.3;
- the application takes appropriate precautions as discussed in the "Resolution" section below.

Resolution

Affected users should upgrade to TF-PSA-Crypto 1.1.0 or above, to Mbed TLS 4.1.0 or above, or to Mbed TLS 3.6.6 or a later 3.6 version. These versions provide two things:

- The new functions `psa_random_reseed()`, `psa_random_deplete()` and `psa_random_set_prediction_resistance()` allow the application to control the reseeding of the PSA random generator.
- The PSA random generator automatically reseeds after a `fork()` call.

In addition, applications should take the following precautions:

- If the application is part of a system image that is cloned, you must trigger a reseed of the random generator after cloning.

- If the application instantiates a legacy random generator using `mbedtls_ctr_drbg_context` or `mbedtls_hmac_drbg_context` objects, you must reseed the random generator after forking or cloning.

See the knowledge base entry Random generator state cloning for more information.

Fix commits

We recommend that users upgrade to a release including the fix. However, if you are maintaining a branch with backported bug fixes, here are the most relevant commits. Please note that these commits may not apply cleanly to older versions of the library, and may not provide a complete fix even if they do apply. The Mbed TLS development team does not provide support outside of maintained branches.

New functions only

The following commits provide the new functions for explicit reseeding. This selection is recommended for platforms where application or system cloning is relevant. Note that on Unix-like systems, with only these commits, applications that call `fork()` need to call these functions as directed.

- Mbed TLS 3.6: a1d7a81d3964b7555255a5a2f5503b3df1523d5e..d05d789316d4797335e3951065c29be4e1c7bb09
- TF-PSA-Crypto 1.0: 125474d4e05965a6dfe2af350b5462ce62bed4cd..e510708536e9a9cdac8367699fa714e7b978b2e7

Fork protection only

The following commits provide automatic protection of the PSA random generator after `fork()`. They are relevant for Unix-like platforms. They do not provide ways for applications to handle other cloning scenarios.

- Mbed TLS 3.6: 168461a3a907941ab73bcd54652516299b32a6e8
  4de8b1043ac7da643a477cb2260018e8d5197615
  fb6503bf62ea5df4dbaaf285c4c03fab4bc05940
  0b93865aed2860c16ee2761543145d0a967759d6
  fd0e168fabb41b703634b13de701a2a4d5bea958
- TF-PSA-Crypto 1.0: 939de010dc9bb59974b02918d30519a0b5ddd5c9
  fb12c309f6889ba4634f9f649696b4b1599c0219
  d57dc99d339e3f967a9874ff9cd445b754ef7dc4
  c3454db1745182786d6eb96c46a969f00c3f445e
  a5e9726f2e6e180a2aa15cffbb640cfa9f661205

Resolve the conflict in `ChangeLog.d/*` by keeping the file deleted (`git rm git rm ChangeLog.d/rng-cloning.txt`).

Additionally, please check that the internal macro is `MBEDTLS_PLATFORM_IS_UNIXLIKE` is getting defined in your build. The definition is in `library/common.h` in the patch for Mbed TLS 3.6 and in `core/tf_psa_crypto_common.h` in the patch for TF-PSA-Crypto 1.0. If your platform declares `fork()` and `getpid()` in `<unistd.h>` but is not recognized as Unix-like, you can add `-DMBEDTLS_PLATFORM_IS_UNIXLIKE` to `CFLAGS` instead of (or in addition to) the first commit listed above.

Complete fix

The following commit ranges provide the complete fix for this vulnerability, including new library functions, automatic protection for `fork()`, documentation and unit tests.

- Mbed TLS 3.6: 168461a3a907941ab73bcd54652516299b32a6e8
  a1d7a81d3964b7555255a5a2f5503b3df1523d5e..d05d789316d4797335e3951065c29be4e1c7bb09
  0764c9348a7712b427c2855c131e1b48720c36b1..fd0e168fabb41b703634b13de701a2a4d5bea958
- TF-PSA-Crypto 1.0: 939de010dc9bb59974b02918d30519a0b5ddd5c9
  125474d4e05965a6dfe2af350b5462ce62bed4cd..e510708536e9a9cdac8367699fa714e7b978b2e7
  e73410ddc234e0d461d91263dd05a22bc34fe8b3..a5e9726f2e6e180a2aa15cffbb640cfa9f661205
- `framework` submodule patches — needed for both consuming branches:
  f41a9f605699bf05cf1e3dcbab26f7f21afec462
  6d5987a9540929f820cbc9b6ff2215f6362fe740
  d1a8b5b59697068f0cd419765ccd3a30cf885d4d..1a5bf10ca08c06be10857c224c5fd70ef38591f2

Resolve the conflict in `ChangeLog.d/*` by keeping the file deleted (`git rm ChangeLog.d/rng-cloning.txt`). Resolve the conflicts in `**/pk_helpers.*` by keeping the file deleted (`git rm tests/include/test/pk_helpers.h tests/src/pk_helpers.c`).