Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-09-08

Recent community activity (thank you!)

- tls#9542 manoel-serafim - Performance Enhancements and Memory Footprint Reduction in mbedtls_internal_sha(256|512)_process_c()
- tls#10377 kraj - x509_crt: Zero-initialize mbedtls_x509_time at declaration
- tls#2748 catenacyber - fuzzing: better corpus for client and server
- tls#10372 dc6jgk - allow negotiation of all use_srtp profile values currently listed by IANA

Recent community activity (thank you!)

Valerio @Nordic

- tls#10333 valeriosetti - [development] Migrate from mbedtls_pk_can_do_ext to mbedtls_pk_can_do_psa (2/2)
- tls#10356 valeriosetti - tests: configuration-crypto: enable p192 curves in test_psa_crypto_without_heap - SHADOW
- crypto#394 valeriosetti - [tf-psa-crypto] Implement mbedtls_pk_can_do_psa (improved mbedtls_pk_can_do_ext) (1/2)
- crypto#408 valeriosetti - [tf-psa-crypto] Remove 224-bit curves (5/6)

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- TF-PSA-Crypto
  - First standalone components are now running in the CI
- Mbed TLS 4.0/TF-PSA-Crypto 1.0
  - Making low level crypto functions internal
  - Removing legacy types from public non-PSA interfaces
  - Removing legacy configuration options
  - PK API for 1.0
  - Released 4.0/1.0 beta for early evaluation

Release Timeline

- 1.0/4.0 code freeze planned for end of September 2025
- 3.6 LTS supported until early 2027
  - 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
  - 3.6.2 (Oct 2024): security fix
  - 3.6.3 (March 2024): supports a PSA key store in builds without malloc
  - 3.6.4 (June 2024): GCC 15 support, other bug and security fixes

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు