Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-09-07

Recent community activity (thank you!)

Mbed TLS

- tls#10941 sridhar-design - PKCS#7: Embedded certificate support and chain verification
- merged: tls#10945 okning - Backport 3.6: Fix getrandom detection with musl libc
- merged: tls#10940 HelloOO7 - Backport 4.1: Restore __cplusplus guard absent from oid.h
- merged: tls#10927 HelloOO7 - Restore __cplusplus guard absent from oid.h
- tls#10911 subotac - Reject overflowing numeric OID components
- tls#10939 v1rtu3x - Backport: Fix missing zeroization in psa_key_agreement()
- tls#10857 vanhauser-thc - new and expanded fuzzing harnesses
- tls#10758 wkhadgar - ssl: size _pms_ecdh against PSA_RAW_KEY_AGREEMENT_OUTPUT_MAX_SIZE
- tls#10936 v1rtu3x - Fix X.509 certificate profiles to honor MBEDTLS_PK_SIGALG_ECDSA
- tls#10934 v1rtu3x - tls13: server: reject zero-length psk_key_exchange_modes
- tls#10932 JulioLoayzaM - Fix PSA initialisation in client fuzzers
- tls#10833 nvxbug - Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- tls#10909 mmustafasenoglu - doc(tls): improve MBEDTLS_ERR_SSL_RECEIVED_NEW_SESSION_TICKET documentation
- tls#10933 mmustafasenoglu - Fix memory errors in sample programs
- merged: tls#10850 AaryanCdry - Backport 3.6: Fix inconsistent docs for mbedtls_sha3_finish and mbedtls_sha3 olen
- tls#10852 felipereyesmurcia - Fix buffer overreads on malformed inputs in sample programs
- tls#10829 mmustafasenoglu - Fix memory errors in sample programs
- tls#10928 nvxbug - Backport 3.6: Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- tls#10929 nvxbug - Backport 4.1: Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest

Recent community activity (thank you!)

TF-PSA-Crypto

- frame#319 sridhar-design - data_files: Add PKCS7 certificate chain and SignedData test files
- frame#317 JulioLoayzaM - Add X.509 fuzzing seeds
- crypto#892 v1rtu3x - Enforce hash length in psa_sign_hash and psa_verify_hash
- merged: crypto#893 okning - Backport 1.1: Fix getrandom detection with musl libc
- merged: crypto#843 okning - Fix getrandom detection with musl libc
- crypto#782 lhuang04 - Fix -Wundef warnings for MBEDTLS_GCC_VERSION in alignment.h
- merged: crypto#886 v1rtu3x - Fix missing zeroization in psa_key_agreement()
- merged: crypto#890 v1rtu3x - Backport 1.1: Fix missing zeroization in psa_key_agreement()
- crypto#865 vanhauser-thc - expand fuzzers, set-up safe fuzzing defaults
- crypto#873 sweetlilmre - constant_time: fix the -Os inlining loss, and add an Xtensa assembly path
- crypto#806 bpcyril-jpg - Revert "include tf_psa_crypto_platform_requirements.h in tf_psa_crypto_config.c"
- crypto#883 JulioLoayzaM - Add Wycheproof tests
- crypto#884 JulioLoayzaM - Add Wycheproof test function for ECDSA
- crypto#885 JulioLoayzaM - Add Wycheproof test function for RSA-PSS
- crypto#880 oubaid-a - Enhance the PSA driver test jinja templates for hashing, AES, signature and key agreement functions
- crypto#810 sigvartmh - SPAKE2+ PSA PAKE API support
- crypto#817 sigvartmh - SPAKE2+: Implement public key import and export

Recent community activity (thank you!)

Valerio (Nordic)

- tls#10642 valeriosetti - Replace legacy rsa symbols followup
- tls#10764 valeriosetti - Allow TF-PSA-Crypto path to be specified in CMake and Makefiles
- frame#316 valeriosetti - Prerequisites for testing Blake2 algorithm in TF-PSA-Crypto
- crypto#867 valeriosetti - Add support for Blake2s and Blake2b hash algorithms

Major activities within core team

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

- ML-DSA integration
  - Priority to bootloader/firmware use cases
- Investigation about adding SM3 and BLAKE2
- Bug bounty program
  - Arm is no longer accepting claims about Mbed TLS, only for TF-PSA-Crypto.

Release Timeline

- 1.x/4.x development
  - 1.2/4.2 released on 2026-07-07
  - 1.3/4.3 targeted for end of September
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.1/4.1.1 released on 2026-07-07
  - 1.1.2/4.1.2 targeted for end of September
- 3.6 LTS supported until early 2027
  - 3.6.7 released on 2026-07-07
  - 3.6.8 targeted for end of September

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు