Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2026-08-10

Recent community activity (thank you!)

Mbed TLS

- tls#10833 nvxbug - Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- tls#10828 ThePseudo - x509_crt: Add initialization to time `now`
- tls#10857 vanhauser-thc - new and expanded fuzzing harnesses
- merged: tls#10854 nvxbug - Backport 4.1: Reject out-of-bounds session ID length in ssl_tls12_session_load
- merged: tls#10791 nvxbug - Reject out-of-bounds session ID length in ssl_tls12_session_load
- merged: tls#10853 nvxbug - Backport 3.6: Reject out-of-bounds session ID length in ssl_tls12_session_load
- tls#10852 felipereyesmurcia - Fix buffer overreads on malformed inputs in sample programs
- tls#10850 AaryanCdry - Backport 3.6: Fix inconsistent docs for mbedtls_sha3_finish and mbedtls_sha3 olen
- tls#10829 mmustafasenoglu - Fix memory errors in sample programs
- tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- frame#315 tpambor - Add support for Key Wrapping using PSA Crypto API

Recent community activity (thank you!)

TF-PSA Crypto

- crypto#866 LeonieReichertABB - Hybrid Public Key Encryption (HPKE) Functionality
- crypto#865 vanhauser-thc - expand fuzzers, set-up safe fuzzing defaults
- crypto#863 tpambor - Add support for key wrapping using PSA Crypto API
- crypto#538 ruiliio - Add support for AES-XTS
- crypto#843 okning - Fix getrandom detection with musl libc
- crypto#837 krish2718 - docs: add WPA3-SAE (PSA Crypto API 1.4) design proposal
- merged: crypto#851 parmi93 - Backport 1.1: Remove pattern constraint from location field
- merged: crypto#720 parmi93 - Remove pattern constraint from location field
- crypto#730 hasheddan - docs: fix broken links between specifications
- crypto#817 sigvartmh - SPAKE2+: Implement public key import and export

Recent community activity (thank you!)

Valerio (Nordic)

- tls#10855 valeriosetti - PKCS5 simplify deps on MBEDTLS_CIPHER_PADDING_PKCS7 + PKCS12 remove test exceptions
- tls#10848 valeriosetti - tests: scripts: remove _reference test components
- merged: tls#10847 valeriosetti - [4.1] Reduce dependencies on private `ecp.h` header
- merged: tls#10814 valeriosetti - Reduce dependencies on private `ecp.h` header
- tls#10764 valeriosetti - Allow TF-PSA-Crypto path to be specified in CMake and Makefiles
- merged: crypto#827 valeriosetti - pk: improve error code failure reporting when RSA public key parsing fails (2/2)
- crypto#864 valeriosetti - PKCS5 simplify deps on MBEDTLS_CIPHER_PADDING_PKCS7 + PKCS12 remove test exceptions
- merged: crypto#853 valeriosetti - [1.1] Inconsistent return value of mbedtls_pk_parse_key breaks mbedtls_pk_check_pair sometimes
- merged: crypto#811 valeriosetti - Inconsistent return value of mbedtls_pk_parse_key breaks mbedtls_pk_check_pair sometimes
- crypto#673 valeriosetti - Only build mbedtls_rsa_deduce_private_exponent when key generation is enabled

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