Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-08-24

Recent community activity (thank you!)

- tls#10833 nvxbug - Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- tls#10758 wkhadgar - ssl: size _pms_ecdh against PSA_RAW_KEY_AGREEMENT_OUTPUT_MAX_SIZE
- tls#10909 mmustafasenoglu - doc(tls): improve MBEDTLS_ERR_SSL_RECEIVED_NEW_SESSION_TICKET documentation
- tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- tls#10840 nzzlinh - Backport v3.6: Fix IAR endianness detection in alignment.h
- tls#10857 vanhauser-thc - new and expanded fuzzing harnesses
- tls#10911 subotac - Reject overflowing numeric OID components
- merged: docs#216 atirna - Replace obsolete gen_key guidance
- crypto#817 sigvartmh - SPAKE2+: Implement public key import and export

Recent community activity (thank you!)

Valerio (Nordic)

- tls#9371 valeriosetti - psasim: use shared memory as messaging system for client-server communication
- tls#10764 valeriosetti - Allow TF-PSA-Crypto path to be specified in CMake and Makefiles
- tls#10642 valeriosetti - Replace legacy rsa symbols followup
- tls#10921 valeriosetti - Prerequisite for adding support for Blake2 in TF-PSA-Crypto
- merged: tls#10848 valeriosetti - tests: scripts: remove _reference test components
- merged: tls#10922 valeriosetti - [1.1] tests: scripts: remove _reference test components
- frame#316 valeriosetti - Prerequisites for testing Blake2 algorithm in TF-PSA-Crypto
- crypto#867 valeriosetti - Add support for Blake2s and Blake2b hash algorithms
- crypto#864 valeriosetti - PKCS5 simplify deps on MBEDTLS_CIPHER_PADDING_PKCS7 + PKCS12 remove test exceptions

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