arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2024-12-16

Recent community activity (thank you!)

- #9849 solardiz - [Backport 2.28] Specify previously missed register clobbers in AES-NI asm blocks
- #9848 solardiz - [Backport 3.6] Specify previously missed register clobbers in AES-NI asm blocks
- #9809 solardiz - Specify previously missed register clobbers in AES-NI asm blocks
- #9421 mfil - Implement TLS-Exporter
- #9839 ucko - psa_wipe_tag_output_buffer: Bail if the buffer is NULL.
- #9797 NadavTasher - Added minimal TLSv1.3-only client configuration
- #9798 NadavTasher - Added debug print in tls13 ssl_tls13_write_key_share_ext
- #9460 krish2718 - Add CNSA presets
- #9777 hughsie - Add a SBOM file in CycloneDX format
- merged: #9810 SuperIlu - Fix compilation on MS-DOS DJGPP
- merged: #9812 SuperIlu - Mbedtls 3.6: Fix compilation on MS-DOS DJGPP
- merged: #9811 SuperIlu - Mbedtls 2.28: Fix compilation on MS-DOS DJGPP
- #8800 winterheart - Allow install headers to different location (mbedtls-3)
- #9825 valeriosetti - Move "easy" basic checks scripts to the framework
- #9826 valeriosetti - [3.6] Move "easy" basic checks scripts to the framework

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/1

- TF-PSA-Crypto — main focus in Q4
  - Splitting files, reworking some interfaces (configuration, platform, …)
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Will become upstream source for crypto in Mbed TLS
- Mbed TLS 4.0
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- Mbed TLS 3.6.2
  - Security fix release (CVE-2024-49195)
- Open for SPAKE2+ reviews (tasks defined on backlog board)

Release Timeline

- 4.0 currently aiming for first half of 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 (TBA): will support a PSA key store in builds without malloc
- 2.28 LTS ends supported life end of 2024

TF-PSA-Crypto 1.0 + Mbed TLS 4.0 highlights

- TLS 1.2: removing finite-field DH, static ECDH, PKCS#1v1.5 RSA encryption, ~~CBC~~
- Crypto: removing PKCS#1v1.5 RSA encryption, DES, EC curves smaller than 250 bits
- Removing all crypto ALT (use PSA drivers instead)
- Removing low-level crypto APIs (use PSA APIs instead)
  - Removing cipher.h; Keeping parts of md.h and pk.h partially as transition layers
  - Removing direct access to bignum/ECC arithmetic
  - Removing direct access to DRBG

arm

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