Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-04-20

Recent community activity (thank you!)

- tls#10672 Maokaman1 - ssl: accept TLS 1.2 rsa_pss_rsae signature schemes
- tls#10697 friedman-ionq - ssl_tls13_server: suppress unused function warning
- tls#10695 valord577 - Fix build warning/error using llvm-mingw
- tls#10674 Maokaman1 - Backport 3.6: ssl: accept TLS 1.2 rsa_pss_rsae signature schemes
- crypto#410 LoveKarlsson - Made alignment typedefs more robust for IAR
- crypto#743 M-Moawad - platform: fix -Wcast-align warnings in memory_buffer_alloc.c
- merged: crypto#723 aescolar - psa_crypto.c: Fix ifdefs to avoid build warning

Recent community activity (thank you!)

Valerio @Nordic

- tls#10650 valeriosetti - library: tls13: add guard for ssl_tls13_client_hello_has_exts()
- tls#10692 valeriosetti - [backport 3.6] platform: fix -Wcast-align warnings in memory_buffer_alloc.c
- merged: tls#10690 valeriosetti - [Backport 3.6] Rename BEFORE_COLON/BC to avoid conflicts
- merged: tls#10679 valeriosetti - [3.6] psa_crypto.c: Fix ifdefs to avoid build warning
- crypto#760 valeriosetti - [backport 1.1] doxygen: use CMake build dir intead of source dir to host generated files
- crypto#718 valeriosetti - doxygen: use CMake build dir intead of source dir to host generated files
- crypto#757 valeriosetti - [backport 1.1] platform: fix -Wcast-align warnings in memory_buffer_alloc.c
- merged: crypto#741 valeriosetti - [1.1] psa_crypto.c: Fix ifdefs to avoid build warning
- crypto#742 valeriosetti - pull_request_template: add field for TF-PSA-Crypto 1.1 branch

Major activities within core team

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

- ML-DSA embedded
- Security issues

Release Timeline

- 1.x/4.x development
  - 1.2.0/4.2.0 (tentative - end of June)
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.0/4.1.0 (March 2026 - released)
  - 1.1.1/4.1.1 (tentative - end of June)
- 3.6 LTS supported until early 2027
  - 3.6.6 (March 2026 - released)
  - 3.6.7 (tentative - end of June)

arm

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