Security Advisories

- Signature Algorithm Injection
- Risk of insufficient protection of serialized session or context data leading to potential memory safety issues (CVE-2026-34877)
- PSA random generator cloning CVE-2026-25835
- Null pointer dereference when setting a distinguished name (CVE-2026-34874)
- Buffer underflow in `x509_inet_pton_ipv6()` (CVE-2026-25833)
- FFDH: lack of contributory behaviour due to improper input validation (CVE-2026-34872)
- Buffer overflow in FFDH public key export (CVE-2026-34875)
- Entropy on Linux can fall back to /dev/urandom (CVE-2026-34871)
- Compiler-induced constant-time violations (CVE-2025-66442)
- Client impersonation while resuming a TLS 1.3 session (CVE-2026-34873)
- CCM multipart finish tag-length validation bypass (CVE-2026-34876)
- Side channel in RSA key generation and operations (SSBleed, M-Step) (CVE-2025-54764)
- Padding oracle through timing of cipher error reporting (CVE-2025-59438)
- Misleading memory management in `mbedtls_x509_string_to_names()`
- NULL pointer dereference after using `mbedtls_asn1_store_named_data()`
- Timing side-channel in block cipher decryption with PKCS#7 padding
- Out-of-bounds read in mbedtls_lms_import_public_key()
- Unchecked return value in LMS verification allows signature bypass
- Heap buffer under-read when parsing PEM-encrypted material
- Race condition in AESNI support detection
- Potential authentication bypass in TLS handshake
- TLS clients may unwittingly skip server authentication
- Buffer underrun in pkwrite when writing an opaque key pair
- Limited authentication bypass in TLS 1.3 optional client authentication
- Stack buffer overflow in ECDSA signature conversion functions
- CTR_DRBG prioritized over HMAC_DRBG as the PSA DRBG
- Insecure handling of shared memory in PSA Crypto APIs
- Buffer overflow in mbedtls_x509_set_extension()
- Timing side channel in private key RSA operations.
- Buffer overflow in TLS handshake parsing with ECDH
- Buffer overread in TLS stream cipher suites
- Buffer overread in DTLS ClientHello parsing
- Double Free in `mbedtls_ssl_set_session()` in an error case.
- Local side channel attack on static Diffie-Hellman with Montgomery curves

- Local side channel attack on RSA
- Protocol weakness in DHE-PSK key exchange
- Local side channel attack on RSA and static Diffie-Hellman
- Local side channel attack on classical CBC decryption in (D)TLS
- Side-channel attack on ECC key import and validation
- Side channel attack on ECDSA
- Cache attack against RSA key import in SGX
- Side channel attack on ECDSA
- Side channel attack on deterministic ECDSA
- Mbed TLS Security Advisory 2018-03
- Mbed TLS Security Advisory 2018-02
- mbed TLS Security Advisory 2018-01
- mbed TLS Security Advisory 2017-02
- mbed TLS Security Advisory 2017-01
- mbed TLS Security Advisory 2015-01
- PolarSSL Security Advisory 2014-04
- PolarSSL Security Advisory 2014-03
- PolarSSL Security Advisory 2014-02
- PolarSSL Security Advisory 2014-01
- PolarSSL Security Advisory 2013-05
- PolarSSL Security Advisory 2013-04
- PolarSSL Security Advisory 2013-03
- PolarSSL Security Advisory 2013-02
- PolarSSL Security Advisory 2013-01
- PolarSSL Security Advisory 2012-01
- PolarSSL Security Advisory 2011-02
- PolarSSL Security Advisory 2011-01