NEWS

This file gives a brief overview of the major changes between each OpenSSL release. For more details please read the CHANGES file.

OpenSSL Releases

OpenSSL 3.0

Major changes between OpenSSL 3.0.1 and OpenSSL 3.0.2 [15 Mar 2022]

- Fixed a bug in the BN_mod_sqrt() function that can cause it to loop forever for non-prime moduli ([CVE-2022-0778])

Major changes between OpenSSL 3.0.0 and OpenSSL 3.0.1 [14 Dec 2021]

- Fixed invalid handling of X509_verify_cert() internal errors in libssl ([CVE-2021-4044])
- Allow fetching an operation from the provider that owns an unexportable key as a fallback if that is still allowed by the property query.

Major changes between OpenSSL 1.1.1 and OpenSSL 3.0.0 [7 sep 2021]

- Enhanced 'openssl list' with many new options.
- Added migration guide to man7.
- Implemented support for fully "pluggable" TLSv1.3 groups.
- Added suport for Kernel TLS (KTLS).
- Changed the license to the Apache License v2.0.
- Moved all variations of the EVP ciphers CAST5, BF, IDEA, SEED, RC2, RC4, RC5, and DES to the legacy provider.
- Moved the EVP digests MD2, MD4, MDC2, WHIRLPOOL and RIPEMD-160 to the legacy provider.
- Added convenience functions for generating asymmetric key pairs.
- Deprecated the `OCSP_REQ_CTX` type and functions.
- Deprecated the `EC_KEY` and `EC_KEY_METHOD` types and functions.
- Deprecated the `RSA` and `RSA_METHOD` types and functions.
- Deprecated the `DSA` and `DSA_METHOD` types and functions.
- Deprecated the `DH` and `DH_METHOD` types and functions.
- Deprecated the `ERR_load_` functions.
- Remove the `RAND_DRBG` API.
- Deprecated the `ENGINE` API.
- Added `OSSL_LIB_CTX`, a libcrypto library context.
- Added various `_ex` functions to the OpenSSL API that support using a non-default `OSSL_LIB_CTX`.
- Interactive mode is removed from the 'openssl' program.
- The X25519, X448, Ed25519, Ed448, SHAKE128 and SHAKE256 algorithms are included in the FIPS provider.

- X509 certificates signed using SHA1 are no longer allowed at security level 1 or higher. The default security level for TLS is 1, so certificates signed using SHA1 are by default no longer trusted to authenticate servers or clients.
- enable-crypto-mdebug and enable-crypto-mdebug-backtrace were mostly disabled; the project uses address sanitize/leak-detect instead.
- Added a Certificate Management Protocol (CMP, RFC 4210) implementation also covering CRMF (RFC 4211) and HTTP transfer (RFC 6712). It is part of the crypto lib and adds a 'cmp' app with a demo configuration. All widely used CMP features are supported for both clients and servers.
- Added a proper HTTP client supporting GET with optional redirection, POST, arbitrary request and response content types, TLS, persistent connections, connections via HTTP(s) proxies, connections and exchange via user-defined BIOs (allowing implicit connections), and timeout checks.
- Added util/check-format.pl for checking adherence to the coding guidelines.
- Added OSSL_ENCODER, a generic encoder API.
- Added OSSL_DECODER, a generic decoder API.
- Added OSSL_PARAM_BLD, an easier to use API to OSSL_PARAM.
- Added error raising macros, ERR_raise() and ERR_raise_data().
- Deprecated ERR_put_error(), ERR_get_error_line(), ERR_get_error_line_data(), ERR_peek_error_line_data(), ERR_peek_last_error_line_data() and ERR_func_error_string().
- Added OSSL_PROVIDER_available(), to check provider availibility.
- Added 'openssl mac' that uses the EVP_MAC API.
- Added 'openssl kdf' that uses the EVP_KDF API.
- Add OPENSSL_info() and 'openssl info' to get built-in data.
- Add support for enabling instrumentation through trace and debug output.
- Changed our version number scheme and set the next major release to 3.0.0
- Added EVP_MAC, an EVP layer MAC API, and a generic EVP_PKEY to EVP_MAC bridge. Supported MACs are: BLAKE2, CMAC, GMAC, HMAC, KMAC, POLY1305 and SIPHASH.
- Removed the heartbeat message in DTLS feature.
- Added EVP_KDF, an EVP layer KDF and PRF API, and a generic EVP_PKEY to EVP_KDF bridge. Supported KDFs are: HKDF, KBKDF, KRB5 KDF, PBKDF2, PKCS12 KDF, SCRYPT, SSH KDF, SSKDF, TLS1 PRF, X9.42 KDF and X9.63 KDF.
- All of the low-level MD2, MD4, MD5, MDC2, RIPEMD160, SHA1, SHA224, SHA256, SHA384, SHA512 and Whirlpool digest functions have been deprecated.
- All of the low-level AES, Blowfish, Camellia, CAST, DES, IDEA, RC2, RC4, RC5 and SEED cipher functions have been deprecated.
- All of the low-level DH, DSA, ECDH, ECDSA and RSA public key functions have been deprecated.
- SSL 3, TLS 1.0, TLS 1.1, and DTLS 1.0 only work at security level 0.
- Added providers, a new pluggability concept that will replace the ENGINE API and ENGINE implementations.

OpenSSL 1.1.1

Major changes between OpenSSL 1.1.1k and OpenSSL 1.1.1l [24 Aug 2021]

- Fixed an SM2 Decryption Buffer Overflow ([CVE-2021-3711])
- Fixed various read buffer overruns processing ASN.1 strings ([CVE-2021-3712])

Major changes between OpenSSL 1.1.1j and OpenSSL 1.1.1k [25 Mar 2021]

- Fixed a problem with verifying a certificate chain when using the X509_V_FLAG_X509_STRICT flag ([CVE-2021-3450])
- Fixed an issue where an OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client ([CVE-2021-3449])

Major changes between OpenSSL 1.1.1i and OpenSSL 1.1.1j [16 Feb 2021]

- Fixed a NULL pointer deref in the X509_issuer_and_serial_hash() function ([CVE-2021-23841])
- Fixed the RSA_padding_check_SSLv23() function and the RSA_SSLV23_PADDING padding mode to correctly check for rollback attacks
- Fixed an overflow in the EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate functions ([CVE-2021-23840])
- Fixed SRP_Calc_client_key so that it runs in constant time

Major changes between OpenSSL 1.1.1h and OpenSSL 1.1.1i [8 Dec 2020]

- Fixed NULL pointer deref in GENERAL_NAME_cmp (CVE-2020-1971)

Major changes between OpenSSL 1.1.1g and OpenSSL 1.1.1h [22 Sep 2020]

- Disallow explicit curve parameters in verifications chains when X509_V_FLAG_X509_STRICT is used
- Enable 'MinProtocol' and 'MaxProtocol' to configure both TLS and DTLS contexts
- Oracle Developer Studio will start reporting deprecation warnings

Major changes between OpenSSL 1.1.1f and OpenSSL 1.1.1g [21 Apr 2020]

- Fixed segmentation fault in SSL_check_chain() (CVE-2020-1967)

Major changes between OpenSSL 1.1.1e and OpenSSL 1.1.1f [31 Mar 2020]

- Revert the unexpected EOF reporting via SSL_ERROR_SSL

Major changes between OpenSSL 1.1.1d and OpenSSL 1.1.1e [17 Mar 2020]

- Fixed an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli (CVE-2019-1551)

Major changes between OpenSSL 1.1.1c and OpenSSL 1.1.1d [10 Sep 2019]

- Fixed a fork protection issue (CVE-2019-1549)
- Fixed a padding oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)
- For built-in EC curves, ensure an EC_GROUP built from the curve name is used even when parsing explicit parameters
- Compute ECC cofactors if not provided during EC_GROUP construction (CVE-2019-1547)
- Early start up entropy quality from the DEVRANDOM seed source has been improved for older Linux systems
- Correct the extended master secret constant on EBCDIC systems
- Use Windows installation paths in the mingw builds (CVE-2019-1552)
- Changed DH_check to accept parameters with order q and 2q subgroups
- Significantly reduce secure memory usage by the randomness pools
- Revert the DEVRANDOM_WAIT feature for Linux systems

Major changes between OpenSSL 1.1.1b and OpenSSL 1.1.1c [28 May 2019]

- Prevent over long nonces in ChaCha20-Poly1305 (CVE-2019-1543)

Major changes between OpenSSL 1.1.1a and OpenSSL 1.1.1b [26 Feb 2019]

- Change the info callback signals for the start and end of a post-handshake message exchange in TLSv1.3.
- Fix a bug in DTLS over SCTP. This breaks interoperability with older versions of OpenSSL like OpenSSL 1.1.0 and OpenSSL 1.0.2.

Major changes between OpenSSL 1.1.1 and OpenSSL 1.1.1a [20 Nov 2018]

- Timing vulnerability in DSA signature generation (CVE-2018-0734)
- Timing vulnerability in ECDSA signature generation (CVE-2018-0735)

Major changes between OpenSSL 1.1.0i and OpenSSL 1.1.1 [11 Sep 2018]

- Support for TLSv1.3 added. The TLSv1.3 implementation includes:
    - Fully compliant implementation of RFC8446 (TLSv1.3) on by default
    - Early data (0-RTT)
    - Post-handshake authentication and key update
    - Middlebox Compatibility Mode
    - TLSv1.3 PSKs
    - Support for all five RFC8446 ciphersuites
    - RSA-PSS signature algorithms (backported to TLSv1.2)
    - Configurable session ticket support
    - Stateless server support
    - Rewrite of the packet construction code for "safer" packet handling
    - Rewrite of the extension handling code For further important information, see the TLS1.3 page in the OpenSSL Wiki.
- Complete rewrite of the OpenSSL random number generator to introduce the following capabilities
    - The default RAND method now utilizes an AES-CTR DRBG according to NIST standard SP 800-90Ar1.
    - Support for multiple DRBG instances with seed chaining.
    - There is a public and private DRBG instance.
    - The DRBG instances are fork-safe.
    - Keep all global DRBG instances on the secure heap if it is enabled.
    - The public and private DRBG instance are per thread for lock free operation
- Support for various new cryptographic algorithms including:
    - SHA3
    - SHA512/224 and SHA512/256
    - EdDSA (both Ed25519 and Ed448) including X509 and TLS support
    - X448 (adding to the existing X25519 support in 1.1.0)
    - Multi-prime RSA
    - SM2
    - SM3
    - SM4
    - SipHash
    - ARIA (including TLS support)
- Significant Side-Channel attack security improvements
- Add a new ClientHello callback to provide the ability to adjust the SSL object at an early stage.
- Add 'Maximum Fragment Length' TLS extension negotiation and support
- A new STORE module, which implements a uniform and URI based reader of stores that can contain keys, certificates, CRLs and numerous other objects.
- Move the display of configuration data to configdata.pm.
- Allow GNU style "make variables" to be used with Configure.

- Claim the namespaces OSSL and OPENSSL, represented as symbol prefixes
- Rewrite of devcrypto engine

OpenSSL 1.1.0

Major changes between OpenSSL 1.1.0k and OpenSSL 1.1.0l [10 Sep 2019]

- Fixed a padding oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)
- For built-in EC curves, ensure an EC_GROUP built from the curve name is used even when parsing explicit parameters
- Compute ECC cofactors if not provided during EC_GROUP construction (CVE-2019-1547)
- Use Windows installation paths in the mingw builds (CVE-2019-1552)

Major changes between OpenSSL 1.1.0j and OpenSSL 1.1.0k [28 May 2019]

- Prevent over long nonces in ChaCha20-Poly1305 (CVE-2019-1543)

Major changes between OpenSSL 1.1.0i and OpenSSL 1.1.0j [20 Nov 2018]

- Timing vulnerability in DSA signature generation (CVE-2018-0734)
- Timing vulnerability in ECDSA signature generation (CVE-2018-0735)

Major changes between OpenSSL 1.1.0h and OpenSSL 1.1.0i [14 Aug 2018]

- Client DoS due to large DH parameter (CVE-2018-0732)
- Cache timing vulnerability in RSA Key Generation (CVE-2018-0737)

Major changes between OpenSSL 1.1.0g and OpenSSL 1.1.0h [27 Mar 2018]

- Constructed ASN.1 types with a recursive definition could exceed the stack (CVE-2018-0739)
- Incorrect CRYPTO_memcmp on HP-UX PA-RISC (CVE-2018-0733)
- rsaz_1024_mul_avx2 overflow bug on x86_64 (CVE-2017-3738)

Major changes between OpenSSL 1.1.0f and OpenSSL 1.1.0g [2 Nov 2017]

- bn_sqrx8x_internal carry bug on x86_64 (CVE-2017-3736)
- Malformed X.509 IPAddressFamily could cause OOB read (CVE-2017-3735)

Major changes between OpenSSL 1.1.0e and OpenSSL 1.1.0f [25 May 2017]

- config now recognises 64-bit mingw and chooses mingw64 instead of mingw

Major changes between OpenSSL 1.1.0d and OpenSSL 1.1.0e [16 Feb 2017]

- Encrypt-Then-Mac renegotiation crash (CVE-2017-3733)

Major changes between OpenSSL 1.1.0c and OpenSSL 1.1.0d [26 Jan 2017]

- Truncated packet could crash via OOB read (CVE-2017-3731)
- Bad (EC)DHE parameters cause a client crash (CVE-2017-3730)
- BN_mod_exp may produce incorrect results on x86_64 (CVE-2017-3732)

Major changes between OpenSSL 1.1.0b and OpenSSL 1.1.0c [10 Nov 2016]

- ChaCha20/Poly1305 heap-buffer-overflow (CVE-2016-7054)
- CMS Null dereference (CVE-2016-7053)
- Montgomery multiplication may produce incorrect results (CVE-2016-7055)

Major changes between OpenSSL 1.1.0a and OpenSSL 1.1.0b [26 Sep 2016]

- Fix Use After Free for large message sizes (CVE-2016-6309)

Major changes between OpenSSL 1.1.0 and OpenSSL 1.1.0a [22 Sep 2016]

- OCSP Status Request extension unbounded memory growth (CVE-2016-6304)
- SSL_peek() hang on empty record (CVE-2016-6305)
- Excessive allocation of memory in tls_get_message_header() (CVE-2016-6307)
- Excessive allocation of memory in dtls1_preprocess_fragment() (CVE-2016-6308)

Major changes between OpenSSL 1.0.2h and OpenSSL 1.1.0 [25 Aug 2016]

- Copyright text was shrunk to a boilerplate that points to the license
- "shared" builds are now the default when possible
- Added support for "pipelining"
- Added the AFALG engine
- New threading API implemented
- Support for ChaCha20 and Poly1305 added to libcrypto and libssl
- Support for extended master secret
- CCM ciphersuites
- Reworked test suite, now based on perl, Test::Harness and Test::More
- *Most* libcrypto and libssl public structures were made opaque, including: BIGNUM and associated types, EC_KEY and EC_KEY_METHOD, DH and DH_METHOD, DSA and DSA_METHOD, RSA and RSA_METHOD, BIO and BIO_METHOD, EVP_MD_CTX, EVP_MD, EVP_CIPHER_CTX, EVP_CIPHER, EVP_PKEY and associated types, HMAC_CTX, X509, X509_CRL, X509_OBJECT, X509_STORE_CTX, X509_STORE, X509_LOOKUP, X509_LOOKUP_METHOD
- libssl internal structures made opaque
- SSLv2 support removed
- Kerberos ciphersuite support removed
- RC4 removed from DEFAULT ciphersuites in libssl
- 40 and 56 bit cipher support removed from libssl
- All public header files moved to include/openssl, no more symlinking
- SSL/TLS state machine, version negotiation and record layer rewritten
- EC revision: now operations use new EC_KEY_METHOD.
- Support for OCB mode added to libcrypto
- Support for asynchronous crypto operations added to libcrypto and libssl
- Deprecated interfaces can now be disabled at build time either relative to the latest release via the "no-deprecated" Configure argument, or via the "--api=1.1.0|1.0.0|0.9.8" option.
- Application software can be compiled with -DOPENSSL_API_COMPAT=version to ensure that features deprecated in that version are not exposed.
- Support for RFC6698/RFC7671 DANE TLSA peer authentication
- Change of Configure to use --prefix as the main installation directory location rather than --openssldir. The latter becomes the directory for certs, private key and openssl.cnf exclusively.
- Reworked BIO networking library, with full support for IPv6.
- New "unified" build system
- New security levels
- Support for scrypt algorithm
- Support for X25519
- Extended SSL_CONF support using configuration files
- KDF algorithm support. Implement TLS PRF as a KDF.
- Support for Certificate Transparency
- HKDF support.

OpenSSL 1.0.2

Major changes between OpenSSL 1.0.2s and OpenSSL 1.0.2t [10 Sep 2019]

- Fixed a padding oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)
- For built-in EC curves, ensure an EC_GROUP built from the curve name is used even when parsing explicit parameters
- Compute ECC cofactors if not provided during EC_GROUP construction (CVE-2019-1547)
- Document issue with installation paths in diverse Windows builds (CVE-2019-1552)

Major changes between OpenSSL 1.0.2r and OpenSSL 1.0.2s [28 May 2019]

- None

Major changes between OpenSSL 1.0.2q and OpenSSL 1.0.2r [26 Feb 2019]

- 0-byte record padding oracle (CVE-2019-1559)

Major changes between OpenSSL 1.0.2p and OpenSSL 1.0.2q [20 Nov 2018]

- Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407)
- Timing vulnerability in DSA signature generation (CVE-2018-0734)

Major changes between OpenSSL 1.0.2o and OpenSSL 1.0.2p [14 Aug 2018]

- Client DoS due to large DH parameter (CVE-2018-0732)
- Cache timing vulnerability in RSA Key Generation (CVE-2018-0737)

Major changes between OpenSSL 1.0.2n and OpenSSL 1.0.2o [27 Mar 2018]

- Constructed ASN.1 types with a recursive definition could exceed the stack (CVE-2018-0739)

Major changes between OpenSSL 1.0.2m and OpenSSL 1.0.2n [7 Dec 2017]

- Read/write after SSL object in error state (CVE-2017-3737)
- rsaz_1024_mul_avx2 overflow bug on x86_64 (CVE-2017-3738)

Major changes between OpenSSL 1.0.2l and OpenSSL 1.0.2m [2 Nov 2017]

- bn_sqrx8x_internal carry bug on x86_64 (CVE-2017-3736)
- Malformed X.509 IPAddressFamily could cause OOB read (CVE-2017-3735)

Major changes between OpenSSL 1.0.2k and OpenSSL 1.0.2l [25 May 2017]

- config now recognises 64-bit mingw and chooses mingw64 instead of mingw

Major changes between OpenSSL 1.0.2j and OpenSSL 1.0.2k [26 Jan 2017]

- Truncated packet could crash via OOB read (CVE-2017-3731)
- BN_mod_exp may produce incorrect results on x86_64 (CVE-2017-3732)
- Montgomery multiplication may produce incorrect results (CVE-2016-7055)

Major changes between OpenSSL 1.0.2i and OpenSSL 1.0.2j [26 Sep 2016]

- Missing CRL sanity check (CVE-2016-7052)

Major changes between OpenSSL 1.0.2h and OpenSSL 1.0.2i [22 Sep 2016]

- OCSP Status Request extension unbounded memory growth (CVE-2016-6304)
- SWEET32 Mitigation (CVE-2016-2183)
- OOB write in MDC2_Update() (CVE-2016-6303)

- Malformed SHA512 ticket DoS (CVE-2016-6302)
- OOB write in BN_bn2dec() (CVE-2016-2182)
- OOB read in TS_OBJ_print_bio() (CVE-2016-2180)
- Pointer arithmetic undefined behaviour (CVE-2016-2177)
- Constant time flag not preserved in DSA signing (CVE-2016-2178)
- DTLS buffered message DoS (CVE-2016-2179)
- DTLS replay protection DoS (CVE-2016-2181)
- Certificate message OOB reads (CVE-2016-6306)

Major changes between OpenSSL 1.0.2g and OpenSSL 1.0.2h [3 May 2016]

- Prevent padding oracle in AES-NI CBC MAC check (CVE-2016-2107)
- Fix EVP_EncodeUpdate overflow (CVE-2016-2105)
- Fix EVP_EncryptUpdate overflow (CVE-2016-2106)
- Prevent ASN.1 BIO excessive memory allocation (CVE-2016-2109)
- EBCDIC overread (CVE-2016-2176)
- Modify behavior of ALPN to invoke callback after SNI/servername callback, such that updates to the SSL_CTX affect ALPN.
- Remove LOW from the DEFAULT cipher list. This removes singles DES from the default.
- Only remove the SSLv2 methods with the no-ssl2-method option.

Major changes between OpenSSL 1.0.2f and OpenSSL 1.0.2g [1 Mar 2016]

- Disable weak ciphers in SSLv3 and up in default builds of OpenSSL.
- Disable SSLv2 default build, default negotiation and weak ciphers (CVE-2016-0800)
- Fix a double-free in DSA code (CVE-2016-0705)
- Disable SRP fake user seed to address a server memory leak (CVE-2016-0798)
- Fix BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797)
- Fix memory issues in BIO_*printf functions (CVE-2016-0799)
- Fix side channel attack on modular exponentiation (CVE-2016-0702)

Major changes between OpenSSL 1.0.2e and OpenSSL 1.0.2f [28 Jan 2016]

- DH small subgroups (CVE-2016-0701)
- SSLv2 doesn't block disabled ciphers (CVE-2015-3197)

Major changes between OpenSSL 1.0.2d and OpenSSL 1.0.2e [3 Dec 2015]

- BN_mod_exp may produce incorrect results on x86_64 (CVE-2015-3193)
- Certificate verify crash with missing PSS parameter (CVE-2015-3194)
- X509_ATTRIBUTE memory leak (CVE-2015-3195)
- Rewrite EVP_DecodeUpdate (base64 decoding) to fix several bugs
- In DSA_generate_parameters_ex, if the provided seed is too short, return an error

Major changes between OpenSSL 1.0.2c and OpenSSL 1.0.2d [9 Jul 2015]

- Alternate chains certificate forgery (CVE-2015-1793)
- Race condition handling PSK identify hint (CVE-2015-3196)

Major changes between OpenSSL 1.0.2b and OpenSSL 1.0.2c [12 Jun 2015]

- Fix HMAC ABI incompatibility

Major changes between OpenSSL 1.0.2a and OpenSSL 1.0.2b [11 Jun 2015]

- Malformed ECParameters causes infinite loop (CVE-2015-1788)
- Exploitable out-of-bounds read in X509_cmp_time (CVE-2015-1789)

- PKCS7 crash with missing EnvelopedContent (CVE-2015-1790)
- CMS verify infinite loop with unknown hash function (CVE-2015-1792)
- Race condition handling NewSessionTicket (CVE-2015-1791)

Major changes between OpenSSL 1.0.2 and OpenSSL 1.0.2a [19 Mar 2015]

- OpenSSL 1.0.2 ClientHello sigalgs DoS fix (CVE-2015-0291)
- Multiblock corrupted pointer fix (CVE-2015-0290)
- Segmentation fault in DTLSv1_listen fix (CVE-2015-0207)
- Segmentation fault in ASN1_TYPE_cmp fix (CVE-2015-0286)
- Segmentation fault for invalid PSS parameters fix (CVE-2015-0208)
- ASN.1 structure reuse memory corruption fix (CVE-2015-0287)
- PKCS7 NULL pointer dereferences fix (CVE-2015-0289)
- DoS via reachable assert in SSLv2 servers fix (CVE-2015-0293)
- Empty CKE with client auth and DHE fix (CVE-2015-1787)
- Handshake with unseeded PRNG fix (CVE-2015-0285)
- Use After Free following d2i_ECPrivatekey error fix (CVE-2015-0209)
- X509_to_X509_REQ NULL pointer deref fix (CVE-2015-0288)
- Removed the export ciphers from the DEFAULT ciphers

Major changes between OpenSSL 1.0.1l and OpenSSL 1.0.2 [22 Jan 2015]

- Suite B support for TLS 1.2 and DTLS 1.2
- Support for DTLS 1.2
- TLS automatic EC curve selection.
- API to set TLS supported signature algorithms and curves
- SSL_CONF configuration API.
- TLS Brainpool support.
- ALPN support.
- CMS support for RSA-PSS, RSA-OAEP, ECDH and X9.42 DH.

OpenSSL 1.0.1

Major changes between OpenSSL 1.0.1t and OpenSSL 1.0.1u [22 Sep 2016]

- OCSP Status Request extension unbounded memory growth (CVE-2016-6304)
- SWEET32 Mitigation (CVE-2016-2183)
- OOB write in MDC2_Update() (CVE-2016-6303)
- Malformed SHA512 ticket DoS (CVE-2016-6302)
- OOB write in BN_bn2dec() (CVE-2016-2182)
- OOB read in TS_OBJ_print_bio() (CVE-2016-2180)
- Pointer arithmetic undefined behaviour (CVE-2016-2177)
- Constant time flag not preserved in DSA signing (CVE-2016-2178)
- DTLS buffered message DoS (CVE-2016-2179)
- DTLS replay protection DoS (CVE-2016-2181)
- Certificate message OOB reads (CVE-2016-6306)

Major changes between OpenSSL 1.0.1s and OpenSSL 1.0.1t [3 May 2016]

- Prevent padding oracle in AES-NI CBC MAC check (CVE-2016-2107)
- Fix EVP_EncodeUpdate overflow (CVE-2016-2105)
- Fix EVP_EncryptUpdate overflow (CVE-2016-2106)
- Prevent ASN.1 BIO excessive memory allocation (CVE-2016-2109)
- EBCDIC overread (CVE-2016-2176)

- Modify behavior of ALPN to invoke callback after SNI/servername callback, such that updates to the SSL_CTX affect ALPN.
- Remove LOW from the DEFAULT cipher list. This removes singles DES from the default.
- Only remove the SSLv2 methods with the no-ssl2-method option.

Major changes between OpenSSL 1.0.1r and OpenSSL 1.0.1s [1 Mar 2016]

- Disable weak ciphers in SSLv3 and up in default builds of OpenSSL.
- Disable SSLv2 default build, default negotiation and weak ciphers (CVE-2016-0800)
- Fix a double-free in DSA code (CVE-2016-0705)
- Disable SRP fake user seed to address a server memory leak (CVE-2016-0798)
- Fix BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797)
- Fix memory issues in BIO_*printf functions (CVE-2016-0799)
- Fix side channel attack on modular exponentiation (CVE-2016-0702)

Major changes between OpenSSL 1.0.1q and OpenSSL 1.0.1r [28 Jan 2016]

- Protection for DH small subgroup attacks
- SSLv2 doesn't block disabled ciphers (CVE-2015-3197)

Major changes between OpenSSL 1.0.1p and OpenSSL 1.0.1q [3 Dec 2015]

- Certificate verify crash with missing PSS parameter (CVE-2015-3194)
- X509_ATTRIBUTE memory leak (CVE-2015-3195)
- Rewrite EVP_DecodeUpdate (base64 decoding) to fix several bugs
- In DSA_generate_parameters_ex, if the provided seed is too short, return an error

Major changes between OpenSSL 1.0.1o and OpenSSL 1.0.1p [9 Jul 2015]

- Alternate chains certificate forgery (CVE-2015-1793)
- Race condition handling PSK identify hint (CVE-2015-3196)

Major changes between OpenSSL 1.0.1n and OpenSSL 1.0.1o [12 Jun 2015]

- Fix HMAC ABI incompatibility

Major changes between OpenSSL 1.0.1m and OpenSSL 1.0.1n [11 Jun 2015]

- Malformed ECParameters causes infinite loop (CVE-2015-1788)
- Exploitable out-of-bounds read in X509_cmp_time (CVE-2015-1789)
- PKCS7 crash with missing EnvelopedContent (CVE-2015-1790)
- CMS verify infinite loop with unknown hash function (CVE-2015-1792)
- Race condition handling NewSessionTicket (CVE-2015-1791)

Major changes between OpenSSL 1.0.1l and OpenSSL 1.0.1m [19 Mar 2015]

- Segmentation fault in ASN1_TYPE_cmp fix (CVE-2015-0286)
- ASN.1 structure reuse memory corruption fix (CVE-2015-0287)
- PKCS7 NULL pointer dereferences fix (CVE-2015-0289)
- DoS via reachable assert in SSLv2 servers fix (CVE-2015-0293)
- Use After Free following d2i_ECPrivatekey error fix (CVE-2015-0209)
- X509_to_X509_REQ NULL pointer deref fix (CVE-2015-0288)
- Removed the export ciphers from the DEFAULT ciphers

Major changes between OpenSSL 1.0.1k and OpenSSL 1.0.1l [15 Jan 2015]

- Build fixes for the Windows and OpenVMS platforms

Major changes between OpenSSL 1.0.1j and OpenSSL 1.0.1k [8 Jan 2015]

- Fix for CVE-2014-3571
- Fix for CVE-2015-0206
- Fix for CVE-2014-3569
- Fix for CVE-2014-3572
- Fix for CVE-2015-0204
- Fix for CVE-2015-0205
- Fix for CVE-2014-8275
- Fix for CVE-2014-3570

Major changes between OpenSSL 1.0.1i and OpenSSL 1.0.1j [15 Oct 2014]

- Fix for CVE-2014-3513
- Fix for CVE-2014-3567
- Mitigation for CVE-2014-3566 (SSL protocol vulnerability)
- Fix for CVE-2014-3568

Major changes between OpenSSL 1.0.1h and OpenSSL 1.0.1i [6 Aug 2014]

- Fix for CVE-2014-3512
- Fix for CVE-2014-3511
- Fix for CVE-2014-3510
- Fix for CVE-2014-3507
- Fix for CVE-2014-3506
- Fix for CVE-2014-3505
- Fix for CVE-2014-3509
- Fix for CVE-2014-5139
- Fix for CVE-2014-3508

Major changes between OpenSSL 1.0.1g and OpenSSL 1.0.1h [5 Jun 2014]

- Fix for CVE-2014-0224
- Fix for CVE-2014-0221
- Fix for CVE-2014-0198
- Fix for CVE-2014-0195
- Fix for CVE-2014-3470
- Fix for CVE-2010-5298

Major changes between OpenSSL 1.0.1f and OpenSSL 1.0.1g [7 Apr 2014]

- Fix for CVE-2014-0160
- Add TLS padding extension workaround for broken servers.
- Fix for CVE-2014-0076

Major changes between OpenSSL 1.0.1e and OpenSSL 1.0.1f [6 Jan 2014]

- Don't include gmt_unix_time in TLS server and client random values
- Fix for TLS record tampering bug (CVE-2013-4353)
- Fix for TLS version checking bug (CVE-2013-6449)
- Fix for DTLS retransmission bug (CVE-2013-6450)

Major changes between OpenSSL 1.0.1d and OpenSSL 1.0.1e [11 Feb 2013]

- Corrected fix for (CVE-2013-0169)

Major changes between OpenSSL 1.0.1c and OpenSSL 1.0.1d [4 Feb 2013]

- Fix renegotiation in TLS 1.1, 1.2 by using the correct TLS version.
- Include the fips configuration module.
- Fix OCSP bad key DoS attack (CVE-2013-0166)
- Fix for SSL/TLS/DTLS CBC plaintext recovery attack (CVE-2013-0169)
- Fix for TLS AESNI record handling flaw (CVE-2012-2686)

Major changes between OpenSSL 1.0.1b and OpenSSL 1.0.1c [10 May 2012]

- Fix TLS/DTLS record length checking bug (CVE-2012-2333)
- Don't attempt to use non-FIPS composite ciphers in FIPS mode.

Major changes between OpenSSL 1.0.1a and OpenSSL 1.0.1b [26 Apr 2012]

- Fix compilation error on non-x86 platforms.
- Make FIPS capable OpenSSL ciphers work in non-FIPS mode.
- Fix SSL_OP_NO_TLSv1_1 clash with SSL_OP_ALL in OpenSSL 1.0.0

Major changes between OpenSSL 1.0.1 and OpenSSL 1.0.1a [19 Apr 2012]

- Fix for ASN1 overflow bug (CVE-2012-2110)
- Workarounds for some servers that hang on long client hellos.
- Fix SEGV in AES code.

Major changes between OpenSSL 1.0.0h and OpenSSL 1.0.1 [14 Mar 2012]

- TLS/DTLS heartbeat support.
- SCTP support.
- RFC 5705 TLS key material exporter.
- RFC 5764 DTLS-SRTP negotiation.
- Next Protocol Negotiation.
- PSS signatures in certificates, requests and CRLs.
- Support for password based recipient info for CMS.
- Support TLS v1.2 and TLS v1.1.
- Preliminary FIPS capability for unvalidated 2.0 FIPS module.
- SRP support.

OpenSSL 1.0.0

Major changes between OpenSSL 1.0.0s and OpenSSL 1.0.0t [3 Dec 2015]

- X509_ATTRIBUTE memory leak ((CVE-2015-3195))
- Race condition handling PSK identify hint (CVE-2015-3196)

Major changes between OpenSSL 1.0.0r and OpenSSL 1.0.0s [11 Jun 2015]

- Malformed ECParameters causes infinite loop (CVE-2015-1788)
- Exploitable out-of-bounds read in X509_cmp_time (CVE-2015-1789)
- PKCS7 crash with missing EnvelopedContent (CVE-2015-1790)
- CMS verify infinite loop with unknown hash function (CVE-2015-1792)
- Race condition handling NewSessionTicket (CVE-2015-1791)

Major changes between OpenSSL 1.0.0q and OpenSSL 1.0.0r [19 Mar 2015]

- Segmentation fault in ASN1_TYPE_cmp fix (CVE-2015-0286)
- ASN.1 structure reuse memory corruption fix (CVE-2015-0287)
- PKCS7 NULL pointer dereferences fix (CVE-2015-0289)
- DoS via reachable assert in SSLv2 servers fix (CVE-2015-0293)

- Use After Free following d2i_ECPrivatekey error fix (CVE-2015-0209)
- X509_to_X509_REQ NULL pointer deref fix (CVE-2015-0288)
- Removed the export ciphers from the DEFAULT ciphers

Major changes between OpenSSL 1.0.0p and OpenSSL 1.0.0q [15 Jan 2015]

- Build fixes for the Windows and OpenVMS platforms

Major changes between OpenSSL 1.0.0o and OpenSSL 1.0.0p [8 Jan 2015]

- Fix for CVE-2014-3571
- Fix for CVE-2015-0206
- Fix for CVE-2014-3569
- Fix for CVE-2014-3572
- Fix for CVE-2015-0204
- Fix for CVE-2015-0205
- Fix for CVE-2014-8275
- Fix for CVE-2014-3570

Major changes between OpenSSL 1.0.0n and OpenSSL 1.0.0o [15 Oct 2014]

- Fix for CVE-2014-3513
- Fix for CVE-2014-3567
- Mitigation for CVE-2014-3566 (SSL protocol vulnerability)
- Fix for CVE-2014-3568

Major changes between OpenSSL 1.0.0m and OpenSSL 1.0.0n [6 Aug 2014]

- Fix for CVE-2014-3510
- Fix for CVE-2014-3507
- Fix for CVE-2014-3506
- Fix for CVE-2014-3505
- Fix for CVE-2014-3509
- Fix for CVE-2014-3508

Known issues in OpenSSL 1.0.0m:

- EAP-FAST and other applications using tls_session_secret_cb won't resume sessions. Fixed in 1.0.0n-dev
- Compilation failure of s3_pkt.c on some platforms due to missing `<limits.h>` include. Fixed in 1.0.0n-dev

Major changes between OpenSSL 1.0.0l and OpenSSL 1.0.0m [5 Jun 2014]

- Fix for CVE-2014-0224
- Fix for CVE-2014-0221
- Fix for CVE-2014-0198
- Fix for CVE-2014-0195
- Fix for CVE-2014-3470
- Fix for CVE-2014-0076
- Fix for CVE-2010-5298

Major changes between OpenSSL 1.0.0k and OpenSSL 1.0.0l [6 Jan 2014]

- Fix for DTLS retransmission bug (CVE-2013-6450)

Major changes between OpenSSL 1.0.0j and OpenSSL 1.0.0k [5 Feb 2013]

- Fix for SSL/TLS/DTLS CBC plaintext recovery attack (CVE-2013-0169)

- Fix OCSP bad key DoS attack (CVE-2013-0166)

Major changes between OpenSSL 1.0.0i and OpenSSL 1.0.0j [10 May 2012]

- Fix DTLS record length checking bug (CVE-2012-2333)

Major changes between OpenSSL 1.0.0h and OpenSSL 1.0.0i [19 Apr 2012]

- Fix for ASN1 overflow bug (CVE-2012-2110)

Major changes between OpenSSL 1.0.0g and OpenSSL 1.0.0h [12 Mar 2012]

- Fix for CMS/PKCS#7 MMA (CVE-2012-0884)
- Corrected fix for (CVE-2011-4619)
- Various DTLS fixes.

Major changes between OpenSSL 1.0.0f and OpenSSL 1.0.0g [18 Jan 2012]

- Fix for DTLS DoS issue (CVE-2012-0050)

Major changes between OpenSSL 1.0.0e and OpenSSL 1.0.0f [4 Jan 2012]

- Fix for DTLS plaintext recovery attack (CVE-2011-4108)
- Clear block padding bytes of SSL 3.0 records (CVE-2011-4576)
- Only allow one SGC handshake restart for SSL/TLS (CVE-2011-4619)
- Check parameters are not NULL in GOST ENGINE (CVE-2012-0027)
- Check for malformed RFC3779 data (CVE-2011-4577)

Major changes between OpenSSL 1.0.0d and OpenSSL 1.0.0e [6 Sep 2011]

- Fix for CRL vulnerability issue (CVE-2011-3207)
- Fix for ECDH crashes (CVE-2011-3210)
- Protection against EC timing attacks.
- Support ECDH ciphersuites for certificates using SHA2 algorithms.
- Various DTLS fixes.

Major changes between OpenSSL 1.0.0c and OpenSSL 1.0.0d [8 Feb 2011]

- Fix for security issue (CVE-2011-0014)

Major changes between OpenSSL 1.0.0b and OpenSSL 1.0.0c [2 Dec 2010]

- Fix for security issue (CVE-2010-4180)
- Fix for (CVE-2010-4252)
- Fix mishandling of absent EC point format extension.
- Fix various platform compilation issues.
- Corrected fix for security issue (CVE-2010-3864).

Major changes between OpenSSL 1.0.0a and OpenSSL 1.0.0b [16 Nov 2010]

- Fix for security issue (CVE-2010-3864).
- Fix for (CVE-2010-2939)
- Fix WIN32 build system for GOST ENGINE.

Major changes between OpenSSL 1.0.0 and OpenSSL 1.0.0a [1 Jun 2010]

- Fix for security issue (CVE-2010-1633).
- GOST MAC and CFB fixes.

Major changes between OpenSSL 0.9.8n and OpenSSL 1.0.0 [29 Mar 2010]

- RFC3280 path validation: sufficient to process PKITS tests.
- Integrated support for PVK files and keyblobs.
- Change default private key format to PKCS#8.
- CMS support: able to process all examples in RFC4134
- Streaming ASN1 encode support for PKCS#7 and CMS.
- Multiple signer and signer add support for PKCS#7 and CMS.
- ASN1 printing support.
- Whirlpool hash algorithm added.
- RFC3161 time stamp support.
- New generalised public key API supporting ENGINE based algorithms.
- New generalised public key API utilities.
- New ENGINE supporting GOST algorithms.
- SSL/TLS GOST ciphersuite support.
- PKCS#7 and CMS GOST support.
- RFC4279 PSK ciphersuite support.
- Supported points format extension for ECC ciphersuites.
- ecdsa-with-SHA224/256/384/512 signature types.
- dsa-with-SHA224 and dsa-with-SHA256 signature types.
- Opaque PRF Input TLS extension support.
- Updated time routines to avoid OS limitations.

OpenSSL 0.9.x

Major changes between OpenSSL 0.9.8m and OpenSSL 0.9.8n [24 Mar 2010]

- CFB cipher definition fixes.
- Fix security issues CVE-2010-0740 and CVE-2010-0433.

Major changes between OpenSSL 0.9.8l and OpenSSL 0.9.8m [25 Feb 2010]

- Cipher definition fixes.
- Workaround for slow RAND_poll() on some WIN32 versions.
- Remove MD2 from algorithm tables.
- SPKAC handling fixes.
- Support for RFC5746 TLS renegotiation extension.
- Compression memory leak fixed.
- Compression session resumption fixed.
- Ticket and SNI coexistence fixes.
- Many fixes to DTLS handling.

Major changes between OpenSSL 0.9.8k and OpenSSL 0.9.8l [5 Nov 2009]

- Temporary work around for CVE-2009-3555: disable renegotiation.

Major changes between OpenSSL 0.9.8j and OpenSSL 0.9.8k [25 Mar 2009]

- Fix various build issues.
- Fix security issues CVE-2009-0590, CVE-2009-0591, CVE-2009-0789

Major changes between OpenSSL 0.9.8i and OpenSSL 0.9.8j [7 Jan 2009]

- Fix security issue (CVE-2008-5077)
- Merge FIPS 140-2 branch code.

Major changes between OpenSSL 0.9.8g and OpenSSL 0.9.8h [28 May 2008]

- CryptoAPI ENGINE support.
- Various precautionary measures.
- Fix for bugs affecting certificate request creation.
- Support for local machine keyset attribute in PKCS#12 files.

Major changes between OpenSSL 0.9.8f and OpenSSL 0.9.8g [19 Oct 2007]

- Backport of CMS functionality to 0.9.8.
- Fixes for bugs introduced with 0.9.8f.

Major changes between OpenSSL 0.9.8e and OpenSSL 0.9.8f [11 Oct 2007]

- Add gcc 4.2 support.
- Add support for AES and SSE2 assembly language optimization for VC++ build.
- Support for RFC4507bis and server name extensions if explicitly selected at compile time.
- DTLS improvements.
- RFC4507bis support.
- TLS Extensions support.

Major changes between OpenSSL 0.9.8d and OpenSSL 0.9.8e [23 Feb 2007]

- Various ciphersuite selection fixes.
- RFC3779 support.

Major changes between OpenSSL 0.9.8c and OpenSSL 0.9.8d [28 Sep 2006]

- Introduce limits to prevent malicious key DoS (CVE-2006-2940)
- Fix security issues CVE-2006-2937, CVE-2006-3737, CVE-2006-4343
- Changes to ciphersuite selection algorithm

Major changes between OpenSSL 0.9.8b and OpenSSL 0.9.8c [5 Sep 2006]

- Fix Daniel Bleichenbacher forged signature attack, CVE-2006-4339
- New cipher Camellia

Major changes between OpenSSL 0.9.8a and OpenSSL 0.9.8b [4 May 2006]

- Cipher string fixes.
- Fixes for VC++ 2005.
- Updated ECC cipher suite support.
- New functions EVP_CIPHER_CTX_new() and EVP_CIPHER_CTX_free().
- Zlib compression usage fixes.
- Built in dynamic engine compilation support on Win32.
- Fixes auto dynamic engine loading in Win32.

Major changes between OpenSSL 0.9.8 and OpenSSL 0.9.8a [11 Oct 2005]

- Fix potential SSL 2.0 rollback (CVE-2005-2969)
- Extended Windows CE support

Major changes between OpenSSL 0.9.7g and OpenSSL 0.9.8 [5 Jul 2005]

- Major work on the BIGNUM library for higher efficiency and to make operations more streamlined and less contradictory. This is the result of a major audit of the BIGNUM library.
- Addition of BIGNUM functions for fields GF(2^m) and NIST curves, to support the Elliptic Crypto functions.
- Major work on Elliptic Crypto; ECDH and ECDSA added, including the use through EVP, X509 and ENGINE.
- New ASN.1 mini-compiler that's usable through the OpenSSL configuration file.
- Added support for ASN.1 indefinite length constructed encoding.

- New PKCS#12 'medium level' API to manipulate PKCS#12 files.
- Complete rework of shared library construction and linking programs with shared or static libraries, through a separate Makefile.shared.
- Rework of the passing of parameters from one Makefile to another.
- Changed ENGINE framework to load dynamic engine modules automatically from specifically given directories.
- New structure and ASN.1 functions for CertificatePair.
- Changed the ZLIB compression method to be stateful.
- Changed the key-generation and primality testing "progress" mechanism to take a structure that contains the ticker function and an argument.
- New engine module: GMP (performs private key exponentiation).
- New engine module: VIA PadLOck ACE extension in VIA C3 Nehemiah processors.
- Added support for IPv6 addresses in certificate extensions. See RFC 1884, section 2.2.
- Added support for certificate policy mappings, policy constraints and name constraints.
- Added support for multi-valued AVAs in the OpenSSL configuration file.
- Added support for multiple certificates with the same subject in the 'openssl ca' index file.
- Make it possible to create self-signed certificates using 'openssl ca -selfsign'.
- Make it possible to generate a serial number file with 'openssl ca -create_serial'.
- New binary search functions with extended functionality.
- New BUF functions.
- New STORE structure and library to provide an interface to all sorts of data repositories. Supports storage of public and private keys, certificates, CRLs, numbers and arbitrary blobs. This library is unfortunately unfinished and unused within OpenSSL.
- New control functions for the error stack.
- Changed the PKCS#7 library to support one-pass S/MIME processing.
- Added the possibility to compile without old deprecated functionality with the OPENSSL_NO_DEPRECATED macro or the 'no-deprecated' argument to the config and Configure scripts.
- Constification of all ASN.1 conversion functions, and other affected functions.
- Improved platform support for PowerPC.
- New FIPS 180-2 algorithms (SHA-224, -256, -384 and -512).
- New X509_VERIFY_PARAM structure to support parameterisation of X.509 path validation.
- Major overhaul of RC4 performance on Intel P4, IA-64 and AMD64.
- Changed the Configure script to have some algorithms disabled by default. Those can be explicitly enabled with the new argument form 'enable-xxx'.
- Change the default digest in 'openssl' commands from MD5 to SHA-1.
- Added support for DTLS.
- New BIGNUM blinding.
- Added support for the RSA-PSS encryption scheme
- Added support for the RSA X.931 padding.
- Added support for BSD sockets on NetWare.
- Added support for files larger than 2GB.
- Added initial support for Win64.
- Added alternate pkg-config files.

Major changes between OpenSSL 0.9.7l and OpenSSL 0.9.7m [23 Feb 2007]

- FIPS 1.1.1 module linking.
- Various ciphersuite selection fixes.

Major changes between OpenSSL 0.9.7k and OpenSSL 0.9.7l [28 Sep 2006]

- Introduce limits to prevent malicious key DoS (CVE-2006-2940)

- Fix security issues CVE-2006-2937, CVE-2006-3737, CVE-2006-4343

Major changes between OpenSSL 0.9.7j and OpenSSL 0.9.7k [5 Sep 2006]

- Fix Daniel Bleichenbacher forged signature attack, CVE-2006-4339

Major changes between OpenSSL 0.9.7i and OpenSSL 0.9.7j [4 May 2006]

- Visual C++ 2005 fixes.
- Update Windows build system for FIPS.

Major changes between OpenSSL 0.9.7h and OpenSSL 0.9.7i [14 Oct 2005]

- Give EVP_MAX_MD_SIZE its old value, except for a FIPS build.

Major changes between OpenSSL 0.9.7g and OpenSSL 0.9.7h [11 Oct 2005]

- Fix SSL 2.0 Rollback (CVE-2005-2969)
- Allow use of fixed-length exponent on DSA signing
- Default fixed-window RSA, DSA, DH private-key operations

Major changes between OpenSSL 0.9.7f and OpenSSL 0.9.7g [11 Apr 2005]

- More compilation issues fixed.
- Adaptation to more modern Kerberos API.
- Enhanced or corrected configuration for Solaris64, Mingw and Cygwin.
- Enhanced x86_64 assembler BIGNUM module.
- More constification.
- Added processing of proxy certificates (RFC 3820).

Major changes between OpenSSL 0.9.7e and OpenSSL 0.9.7f [22 Mar 2005]

- Several compilation issues fixed.
- Many memory allocation failure checks added.
- Improved comparison of X509 Name type.
- Mandatory basic checks on certificates.
- Performance improvements.

Major changes between OpenSSL 0.9.7d and OpenSSL 0.9.7e [25 Oct 2004]

- Fix race condition in CRL checking code.
- Fixes to PKCS#7 (S/MIME) code.

Major changes between OpenSSL 0.9.7c and OpenSSL 0.9.7d [17 Mar 2004]

- Security: Fix Kerberos ciphersuite SSL/TLS handshaking bug
- Security: Fix null-pointer assignment in do_change_cipher_spec()
- Allow multiple active certificates with same subject in CA index
- Multiple X509 verification fixes
- Speed up HMAC and other operations

Major changes between OpenSSL 0.9.7b and OpenSSL 0.9.7c [30 Sep 2003]

- Security: fix various ASN1 parsing bugs.
- New -ignore_err option to OCSP utility.
- Various interop and bug fixes in S/MIME code.
- SSL/TLS protocol fix for unrequested client certificates.

Major changes between OpenSSL 0.9.7a and OpenSSL 0.9.7b [10 Apr 2003]

- Security: counter the Klima-Pokorny-Rosa extension of Bleichbacher's attack
- Security: make RSA blinding default.
- Configuration: Irix fixes, AIX fixes, better mingw support.
- Support for new platforms: linux-ia64-ecc.
- Build: shared library support fixes.
- ASN.1: treat domainComponent correctly.
- Documentation: fixes and additions.

Major changes between OpenSSL 0.9.7 and OpenSSL 0.9.7a [19 Feb 2003]

- Security: Important security related bugfixes.
- Enhanced compatibility with MIT Kerberos.
- Can be built without the ENGINE framework.
- IA32 assembler enhancements.
- Support for new platforms: FreeBSD/IA64 and FreeBSD/Sparc64.
- Configuration: the no-err option now works properly.
- SSL/TLS: now handles manual certificate chain building.
- SSL/TLS: certain session ID malfunctions corrected.

Major changes between OpenSSL 0.9.6 and OpenSSL 0.9.7 [30 Dec 2002]

- New library section OCSP.
- Complete rewrite of ASN1 code.
- CRL checking in verify code and openssl utility.
- Extension copying in 'ca' utility.
- Flexible display options in 'ca' utility.
- Provisional support for international characters with UTF8.
- Support for external crypto devices ('engine') is no longer a separate distribution.
- New elliptic curve library section.
- New AES (Rijndael) library section.
- Support for new platforms: Windows CE, Tandem OSS, A/UX, AIX 64-bit, Linux x86_64, Linux 64-bit on Sparc v9
- Extended support for some platforms: VxWorks
- Enhanced support for shared libraries.
- Now only builds PIC code when shared library support is requested.
- Support for pkg-config.
- Lots of new manuals.
- Makes symbolic links to or copies of manuals to cover all described functions.
- Change DES API to clean up the namespace (some applications link also against libdes providing similar functions having the same name). Provide macros for backward compatibility (will be removed in the future).
- Unify handling of cryptographic algorithms (software and engine) to be available via EVP routines for asymmetric and symmetric ciphers.
- NCONF: new configuration handling routines.
- Change API to use more 'const' modifiers to improve error checking and help optimizers.
- Finally remove references to RSAref.
- Reworked parts of the BIGNUM code.
- Support for new engines: Broadcom ubsec, Accelerated Encryption Processing, IBM 4758.
- A few new engines added in the demos area.
- Extended and corrected OID (object identifier) table.
- PRNG: query at more locations for a random device, automatic query for EGD style random sources at several locations.

- SSL/TLS: allow optional cipher choice according to server's preference.
- SSL/TLS: allow server to explicitly set new session ids.
- SSL/TLS: support Kerberos cipher suites (RFC2712). Only supports MIT Kerberos for now.
- SSL/TLS: allow more precise control of renegotiations and sessions.
- SSL/TLS: add callback to retrieve SSL/TLS messages.
- SSL/TLS: support AES cipher suites (RFC3268).

Major changes between OpenSSL 0.9.6j and OpenSSL 0.9.6k [30 Sep 2003]

- Security: fix various ASN1 parsing bugs.
- SSL/TLS protocol fix for unrequested client certificates.

Major changes between OpenSSL 0.9.6i and OpenSSL 0.9.6j [10 Apr 2003]

- Security: counter the Klima-Pokorny-Rosa extension of Bleichbacher's attack
- Security: make RSA blinding default.
- Build: shared library support fixes.

Major changes between OpenSSL 0.9.6h and OpenSSL 0.9.6i [19 Feb 2003]

- Important security related bugfixes.

Major changes between OpenSSL 0.9.6g and OpenSSL 0.9.6h [5 Dec 2002]

- New configuration targets for Tandem OSS and A/UX.
- New OIDs for Microsoft attributes.
- Better handling of SSL session caching.
- Better comparison of distinguished names.
- Better handling of shared libraries in a mixed GNU/non-GNU environment.
- Support assembler code with Borland C.
- Fixes for length problems.
- Fixes for uninitialised variables.
- Fixes for memory leaks, some unusual crashes and some race conditions.
- Fixes for smaller building problems.
- Updates of manuals, FAQ and other instructive documents.

Major changes between OpenSSL 0.9.6f and OpenSSL 0.9.6g [9 Aug 2002]

- Important building fixes on Unix.

Major changes between OpenSSL 0.9.6e and OpenSSL 0.9.6f [8 Aug 2002]

- Various important bugfixes.

Major changes between OpenSSL 0.9.6d and OpenSSL 0.9.6e [30 Jul 2002]

- Important security related bugfixes.
- Various SSL/TLS library bugfixes.

Major changes between OpenSSL 0.9.6c and OpenSSL 0.9.6d [9 May 2002]

- Various SSL/TLS library bugfixes.
- Fix DH parameter generation for 'non-standard' generators.

Major changes between OpenSSL 0.9.6b and OpenSSL 0.9.6c [21 Dec 2001]

- Various SSL/TLS library bugfixes.
- BIGNUM library fixes.
- RSA OAEP and random number generation fixes.

- Object identifiers corrected and added.
- Add assembler BN routines for IA64.
- Add support for OS/390 Unix, UnixWare with gcc, OpenUNIX 8, MIPS Linux; shared library support for Irix, HP-UX.
- Add crypto accelerator support for AEP, Baltimore SureWare, Broadcom and Cryptographic Appliance's keyserver [in 0.9.6c-engine release].

Major changes between OpenSSL 0.9.6a and OpenSSL 0.9.6b [9 Jul 2001]

- Security fix: PRNG improvements.
- Security fix: RSA OAEP check.
- Security fix: Reinsert and fix countermeasure to Bleichbacher's attack.
- MIPS bug fix in BIGNUM.
- Bug fix in "openssl enc".
- Bug fix in X.509 printing routine.
- Bug fix in DSA verification routine and DSA S/MIME verification.
- Bug fix to make PRNG thread-safe.
- Bug fix in RAND_file_name().
- Bug fix in compatibility mode trust settings.
- Bug fix in blowfish EVP.
- Increase default size for BIO buffering filter.
- Compatibility fixes in some scripts.

Major changes between OpenSSL 0.9.6 and OpenSSL 0.9.6a [5 Apr 2001]

- Security fix: change behavior of OpenSSL to avoid using environment variables when running as root.
- Security fix: check the result of RSA-CRT to reduce the possibility of deducing the private key from an incorrectly calculated signature.
- Security fix: prevent Bleichenbacher's DSA attack.
- Security fix: Zero the premaster secret after deriving the master secret in DH ciphersuites.
- Reimplement SSL_peek(), which had various problems.
- Compatibility fix: the function des_encrypt() renamed to des_encrypt1() to avoid clashes with some Unixen libc.
- Bug fixes for Win32, HP/UX and Irix.
- Bug fixes in BIGNUM, SSL, PKCS#7, PKCS#12, X.509, CONF and memory checking routines.
- Bug fixes for RSA operations in threaded environments.
- Bug fixes in misc. openssl applications.
- Remove a few potential memory leaks.
- Add tighter checks of BIGNUM routines.
- Shared library support has been reworked for generality.
- More documentation.
- New function BN_rand_range().
- Add "-rand" option to openssl s_client and s_server.

Major changes between OpenSSL 0.9.5a and OpenSSL 0.9.6 [10 Oct 2000]

- Some documentation for BIO and SSL libraries.
- Enhanced chain verification using key identifiers.
- New sign and verify options to 'dgst' application.
- Support for DER and PEM encoded messages in 'smime' application.
- New 'rsautl' application, low-level RSA utility.
- MD4 now included.
- Bugfix for SSL rollback padding check.

- Support for external crypto devices [1].
- Enhanced EVP interface.

[1] The support for external crypto devices is currently a separate distribution. See the file README-Engine.md.

Major changes between OpenSSL 0.9.5 and OpenSSL 0.9.5a [1 Apr 2000]

- Bug fixes for Win32, SuSE Linux, NeXTSTEP and FreeBSD 2.2.8
- Shared library support for HPUX and Solaris-gcc
- Support of Linux/IA64
- Assembler support for Mingw32
- New 'rand' application
- New way to check for existence of algorithms from scripts

Major changes between OpenSSL 0.9.4 and OpenSSL 0.9.5 [25 May 2000]

- S/MIME support in new 'smime' command
- Documentation for the OpenSSL command line application
- Automation of 'req' application
- Fixes to make s_client, s_server work under Windows
- Support for multiple fieldnames in SPKACs
- New SPKAC command line utility and associated library functions
- Options to allow passwords to be obtained from various sources
- New public key PEM format and options to handle it
- Many other fixes and enhancements to command line utilities
- Usable certificate chain verification
- Certificate purpose checking
- Certificate trust settings
- Support of authority information access extension
- Extensions in certificate requests
- Simplified X509 name and attribute routines
- Initial (incomplete) support for international character sets
- New DH_METHOD, DSA_METHOD and enhanced RSA_METHOD
- Read only memory BIOs and simplified creation function
- TLS/SSL protocol bugfixes: Accept TLS 'client hello' in SSL 3.0 record; allow fragmentation and interleaving of handshake and other data
- TLS/SSL code now "tolerates" MS SGC
- Work around for Netscape client certificate hang bug
- RSA_NULL option that removes RSA patent code but keeps other RSA functionality
- Memory leak detection now allows applications to add extra information via a per-thread stack
- PRNG robustness improved
- EGD support
- BIGNUM library bug fixes
- Faster DSA parameter generation
- Enhanced support for Alpha Linux
- Experimental macOS support

Major changes between OpenSSL 0.9.3 and OpenSSL 0.9.4 [9 Aug 1999]

- Transparent support for PKCS#8 format private keys: these are used by several software packages and are more secure than the standard form
- PKCS#5 v2.0 implementation
- Password callbacks have a new void * argument for application data
- Avoid various memory leaks

- New pipe-like BIO that allows using the SSL library when actual I/O must be handled by the application (BIO pair)

Major changes between OpenSSL 0.9.2b and OpenSSL 0.9.3 [24 May 1999]

- Lots of enhancements and cleanups to the Configuration mechanism
- RSA OEAP related fixes
- Added "openssl ca -revoke" option for revoking a certificate
- Source cleanups: const correctness, type-safe stacks and ASN.1 SETs
- Source tree cleanups: removed lots of obsolete files
- Thawte SXNet, certificate policies and CRL distribution points extension support
- Preliminary (experimental) S/MIME support
- Support for ASN.1 UTF8String and VisibleString
- Full integration of PKCS#12 code
- Sparc assembler bignum implementation, optimized hash functions
- Option to disable selected ciphers

Major changes between OpenSSL 0.9.1c and OpenSSL 0.9.2b [22 Mar 1999]

- Fixed a security hole related to session resumption
- Fixed RSA encryption routines for the p < q case
- "ALL" in cipher lists now means "everything except NULL ciphers"
- Support for Triple-DES CBCM cipher
- Support of Optimal Asymmetric Encryption Padding (OAEP) for RSA
- First support for new TLSv1 ciphers
- Added a few new BIOs (syslog BIO, reliable BIO)
- Extended support for DSA certificate/keys.
- Extended support for Certificate Signing Requests (CSR)
- Initial support for X.509v3 extensions
- Extended support for compression inside the SSL record layer
- Overhauled Win32 builds
- Cleanups and fixes to the Big Number (BN) library
- Support for ASN.1 GeneralizedTime
- Splitted ASN.1 SETs from SEQUENCEs
- ASN1 and PEM support for Netscape Certificate Sequences
- Overhauled Perl interface
- Lots of source tree cleanups.
- Lots of memory leak fixes.
- Lots of bug fixes.

Major changes between SSLeay 0.9.0b and OpenSSL 0.9.1c [23 Dec 1998]

- Integration of the popular NO_RSA/NO_DSA patches
- Initial support for compression inside the SSL record layer
- Added BIO proxy and filtering functionality
- Extended Big Number (BN) library
- Added RIPE MD160 message digest
- Added support for RC2/64bit cipher
- Extended ASN.1 parser routines
- Adjustments of the source tree for CVS
- Support for various new platforms