Features and bug fixes in OpenSSL from 0.9.7e (WR-SSL base) to 1.0.1o

Version tree from 0.9.7e to 1.0.1o is through following successions:

Version start-end	Major Features/fixes	Comments
0.9.7e to 0.9.7g	**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 0.9.7f 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).	
0.9.7g and 0.9.8	• 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 withing 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 parametrisation 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 explicitely 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.	
0.9.8 to 0.9.8n	**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 0.9.8a 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 0.9.8b and OpenSSL 0.9.8c [5 Sep 2006]:

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

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

- Various ciphersuite selection fixes.
- RFC3779 support.

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 lanugauge 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 0.9.8f 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 0.9.8g 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 0.9.8i and OpenSSL 0.9.8j [7 Jan 2009]:** • Fix security issue (**CVE-2008-5077**) • Merge FIPS 140-2 branch code. **Major changes between OpenSSL 0.9.8j 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 0.9.8k and OpenSSL 0.9.8l [5 Nov 2009]:** • Temporary work around for **CVE-2009-3555**: disable renegotiation. **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 0.9.8m and OpenSSL 0.9.8n [24 Mar 2010]:** • CFB cipher definition fixes. • Fix security issues **CVE-2010-0740** and **CVE-2010-0433**.	
0.9.8n and 1.0.0	• 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.	
1.0.0 to 1.0.0h	**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 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 1.0.0b 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 1.0.0c and OpenSSL 1.0.0d [8 Feb 2011]:

- Fix for security issue **CVE-2011-0014**

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 1.0.0e 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 1.0.0f and OpenSSL 1.0.0g [18 Jan 2012]:

	• Fix for DTLS DoS issue **CVE-2012-0050** **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.	
1.0.0h and 1.0.1	• 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.	
1.0.1 to 1.0.1o	**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 1.0.1a 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 1.0.1b 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 1.0.1c 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 1.0.1d and OpenSSL 1.0.1e [11 Feb 2013]:** • Corrected fix for **CVE-2013-0169** **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 1.0.1f 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 1.0.1g 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 1.0.1h 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 1.0.1i 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 1.0.1j 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 1.0.1k and OpenSSL 1.0.1l [15 Jan 2015]** • Build fixes for the Windows and OpenVMS platforms **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 1.0.1m 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 1.0.1n and OpenSSL 1.0.1o [12 Jun 2015]** • Fix HMAC ABI incompatibility	