|  |  |  |
| --- | --- | --- |
| Certainty | : | **Out-of-date version(OpenSSL)** |
| URL | : | <https://zero.webappsecurity.com/> |
| Identified Version | : | 0.9.8e |
| Latest Version | : | 3.0.1 (in this branch) |
| Vulnerability Database | : | Result is based on 02/16/2022 20:30:00 vulnerability database content. |

CLASSIFICATION

|  |  |
| --- | --- |
| PCI DSS 3.2 | [6.2](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss) |
| OWASP 2013 | [A9](http://www.owasp.org/index.php/Top_10_2013-A9) |
| OWASP 2017 | [A9](https://www.owasp.org/index.php/Top_10_2017-A9) |
| CWE | [829](http://cwe.mitre.org/data/definitions/829.html) |
| CAPEC | [310](http://capec.mitre.org/data/definitions/310.html) |
| HIPAA | [164.308(A)(1)(I)](http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf) |
| ISO27001 | [A.14.1.2](https://www.netsparker.com/compliance-reports/iso27001/control-objectives-and-controls/#A-14-1-2) |

Vulnerability Details

Netsparker identified you are using an out-of-date version of OpenSSL.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of OpenSSL to the latest stable version.

Remedy References

[OpenSSL Project](https://www.openssl.org/)

Known Vulnerabilities in this Version

OpenSSL Resource Management Errors Vulnerability

d1\_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

Affected Versions

0.9.8 to 0.9.8y

External References

[CVE-2014-3506](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3506)

OpenSSL Other Vulnerability

Double free vulnerability in d1\_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

Affected Versions

0.9.8 to 0.9.8y

External References

[CVE-2014-3505](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3505)

OpenSSL Cryptographic Issues Vulnerability

The ssl3\_send\_client\_key\_exchange function in s3\_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Versions

0.9.8 to 0.9.8x

External References

[CVE-2014-3470](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3470)

OpenSSL Cryptographic Issues Vulnerability

The ssl3\_send\_client\_key\_exchange function in s3\_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

Affected Versions

0.9.2b to 0.9.8y

External References

[CVE-2014-3470](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3470)

OpenSSL Inadequate Encryption Strength Vulnerability

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

Affected Versions

0.9.2b to 0.9.8z

External References

[CVE-2014-0224](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224)

OpenSSL Resource Management Errors Vulnerability

Memory leak in d1\_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

Affected Versions

0.9.8 to 0.9.8y

External References

[CVE-2014-3507](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3507)

OpenSSL Other Vulnerability

The ssl3\_send\_client\_key\_exchange function in s3\_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

Affected Versions

0.9.8 to 0.9.8y

External References

[CVE-2014-3510](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3510)

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The OBJ\_obj2txt function in crypto/objects/obj\_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509\_name\_oneline, X509\_name\_print\_ex, and unspecified other functions.

Affected Versions

0.9.8 to 0.9.8y

External References

[CVE-2014-3508](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3508)

OpenSSL Resource Management Errors Vulnerability

The dtls1\_get\_message\_fragment function in d1\_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Versions

0.9.8 to 0.9.8x

External References

[CVE-2014-0221](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0221)

OpenSSL Resource Management Errors Vulnerability

The dtls1\_get\_message\_fragment function in d1\_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

Affected Versions

0.9.2b to 0.9.8y

External References

[CVE-2014-0221](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0221)

OpenSSL Cryptographic Issues Vulnerability

The ssl\_get\_algorithm2 function in ssl/s3\_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2013-6449](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-6449)

OpenSSL Cryptographic Issues Vulnerability

The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

Affected Versions

0.9.8 to 0.9.8x

External References

[CVE-2013-0169](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0169)

OpenSSL Cryptographic Issues Vulnerability

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2014-0076](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0076)

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

Affected Versions

0.9.2b to 0.9.8x

External References

[CVE-2013-0166](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0166)

OpenSSL Permissions, Privileges, and Access Controls Vulnerability

\*\* DISPUTED \*\* OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than [CVE-2011-5094](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5094). NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Affected Versions

0.9.2b to 0.9.8k

External References

[CVE-2011-1473](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1473)

OpenSSL Cryptographic Issues Vulnerability

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

Affected Versions

0.9.2b to 0.9.8y

External References

[CVE-2014-0076](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0076)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1\_reassemble\_fragment function in d1\_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Versions

0.9.8 to 0.9.8x

External References

[CVE-2014-0195](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0195)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1\_reassemble\_fragment function in d1\_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

Affected Versions

0.9.2b to 0.9.8y

External References

[CVE-2014-0195](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0195)

OpenSSL Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the ssl3\_read\_bytes function in s3\_pkt.c in OpenSSL through 1.0.1g, when SSL\_MODE\_RELEASE\_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Versions

0.9.2b to 0.9.8y

External References

[CVE-2010-5298](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5298)

OpenSSL Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the ssl3\_read\_bytes function in s3\_pkt.c in OpenSSL through 1.0.1g, when SSL\_MODE\_RELEASE\_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2010-5298](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5298)

OpenSSL Cryptographic Issues Vulnerability

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Affected Versions

0.9.8 to 0.9.8zb

External References

[CVE-2014-3566](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566)

OpenSSL Other Vulnerability

The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7\_doit.c and crypto/pkcs7/pk7\_lib.c.

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2015-0289](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0289)

OpenSSL Other Vulnerability

The X509\_to\_X509\_REQ function in crypto/x509/x509\_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2015-0288](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0288)

OpenSSL DEPRECATED: Code Vulnerability

The ASN1\_item\_ex\_d2i function in crypto/asn1/tasn\_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2015-0287](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0287)

OpenSSL DEPRECATED: Code Vulnerability

The ASN1\_TYPE\_cmp function in crypto/asn1/a\_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2015-0286](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0286)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1\_clear\_queues function in ssl/d1\_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

Affected Versions

0.9.2b to 0.9.8z

External References

[CVE-2014-8176](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8176)

OpenSSL Cryptographic Issues Vulnerability

The TLS protocol 1.2 and earlier, when a DHE\_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE\_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE\_EXPORT and then rewriting a ServerHello with DHE\_EXPORT replaced by DHE, aka the "Logjam" issue.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2015-4000](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000)

OpenSSL Improper Input Validation Vulnerability

The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2\_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2015-0293](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0293)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Integer underflow in the EVP\_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.

Affected Versions

0.9.2b to 0.9.8z

External References

[CVE-2015-0292](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0292)

OpenSSL Other Vulnerability

Use-after-free vulnerability in the d2i\_ECPrivateKey function in crypto/ec/ec\_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2015-0209](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0209)

OpenSSL Other Vulnerability

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1\_get\_record function in d1\_pkt.c and the ssl3\_read\_n function in s3\_pkt.c.

Affected Versions

0.9.2b to 0.9.8zc

External References

[CVE-2014-3571](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3571)

OpenSSL Cryptographic Issues Vulnerability

The BN\_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86\_64-gcc.c, and crypto/bn/bn\_asm.c.

Affected Versions

0.9.2b to 0.9.8zc

External References

[CVE-2014-3570](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3570)

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23\_clnt.c and s23\_srvr.c.

Affected Versions

0.9.2b to 0.9.8zb

External References

[CVE-2014-3568](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3568)

OpenSSL Improper Input Validation Vulnerability

Memory leak in the tls\_decrypt\_ticket function in t1\_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

Affected Versions

0.9.2b to 0.9.8zb

External References

[CVE-2014-3567](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3567)

OpenSSL Cryptographic Issues Vulnerability

The ssl3\_get\_key\_exchange function in s3\_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.

Affected Versions

0.9.2b to 0.9.8zc

External References

[CVE-2014-3572](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3572)

OpenSSL Cryptographic Issues Vulnerability

The ssl3\_get\_key\_exchange function in s3\_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT\_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT\_RSA issues associated with servers or other TLS implementations.

Affected Versions

0.9.2b to 0.9.8zc

External References

[CVE-2015-0204](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204)

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a\_verify.c, crypto/dsa/dsa\_asn1.c, crypto/ecdsa/ecs\_vrf.c, and crypto/x509/x\_all.c.

Affected Versions

0.9.2b to 0.9.8zc

External References

[CVE-2014-8275](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8275)

OpenSSL Numeric Errors Vulnerability

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

Affected Versions

0.9.2b to 0.9.8v

External References

[CVE-2012-2333](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2333)

OpenSSL Numeric Errors Vulnerability

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

Affected Versions

0.9.2b to 0.9.8w

External References

[CVE-2012-2333](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2333)

OpenSSL Resource Management Errors Vulnerability

The dtls1\_retrieve\_buffered\_fragment function in ssl/d1\_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug."

Affected Versions

0.9.7a to 0.9.8k

External References

[CVE-2009-1387](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1387)

OpenSSL Other Vulnerability

ssl/s3\_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.

Affected Versions

0.9.7a to 0.9.8h

External References

[CVE-2009-1386](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1386)

OpenSSL Resource Management Errors Vulnerability

Multiple memory leaks in the dtls1\_process\_out\_of\_seq\_message function in ssl/d1\_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."

Affected Versions

0.9.8a to 0.9.8j

External References

[CVE-2009-1378](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1378)

OpenSSL Resource Management Errors Vulnerability

Multiple memory leaks in the dtls1\_process\_out\_of\_seq\_message function in ssl/d1\_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."

Affected Versions

0.9.2b to 0.9.8k

External References

[CVE-2009-1378](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1378)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1\_buffer\_record function in ssl/d1\_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."

Affected Versions

0.9.8a to 0.9.8j

External References

[CVE-2009-1377](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1377)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1\_buffer\_record function in ssl/d1\_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."

Affected Versions

0.9.2b to 0.9.8k

External References

[CVE-2009-1377](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1377)

OpenSSL Numeric Errors Vulnerability

OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.

Affected Versions

0.9.2b to 0.9.8i

External References

[CVE-2009-0789](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0789)

OpenSSL Numeric Errors Vulnerability

OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.

Affected Versions

0.9.2b to 0.9.8j

External References

[CVE-2009-0789](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0789)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The ASN1\_STRING\_print\_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.

Affected Versions

0.9.2b to 0.9.8j

External References

[CVE-2009-0590](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0590)

OpenSSL Improper Input Validation Vulnerability

OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP\_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

Affected Versions

0.9.8 to 0.9.8g

External References

[CVE-2008-5077](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5077)

OpenSSL Cryptographic Issues Vulnerability

The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms\_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

Affected Versions

0.9.2b to 0.9.8n

External References

[CVE-2010-0742](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0742)

OpenSSL Improper Input Validation Vulnerability

The kssl\_keytab\_is\_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.

Affected Versions

0.9.8 to 0.9.8l

External References

[CVE-2010-0433](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0433)

OpenSSL Improper Input Validation Vulnerability

The kssl\_keytab\_is\_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.

Affected Versions

0.9.2b to 0.9.8m

External References

[CVE-2010-0433](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0433)

OpenSSL Improper Input Validation Vulnerability

OpenSSL before 0.9.8m does not check for a NULL return value from bn\_wexpand function calls in (1) crypto/bn/bn\_div.c, (2) crypto/bn/bn\_gf2m.c, (3) crypto/ec/ec2\_smpl.c, and (4) engines/e\_ubsec.c, which has unspecified impact and context-dependent attack vectors.

Affected Versions

0.9.8 to 0.9.8k

External References

[CVE-2009-3245](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3245)

OpenSSL Improper Input Validation Vulnerability

OpenSSL before 0.9.8m does not check for a NULL return value from bn\_wexpand function calls in (1) crypto/bn/bn\_div.c, (2) crypto/bn/bn\_gf2m.c, (3) crypto/ec/ec2\_smpl.c, and (4) engines/e\_ubsec.c, which has unspecified impact and context-dependent attack vectors.

Affected Versions

0.9.2b to 0.9.8l

External References

[CVE-2009-3245](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3245)

OpenSSL Resource Management Errors Vulnerability

Memory leak in the zlib\_stateful\_finish function in crypto/comp/c\_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO\_cleanup\_all\_ex\_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to [CVE-2008-1678](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1678).

Affected Versions

0.9.2b to 0.9.8l

External References

[CVE-2009-4355](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4355)

OpenSSL Cryptographic Issues Vulnerability

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod\_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

Affected Versions

0.9.2b to 0.9.8k

External References

[CVE-2009-3555](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3555)

OpenSSL Cryptographic Issues Vulnerability

The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.

Affected Versions

0.9.8 to 0.9.8k

External References

[CVE-2009-2409](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2409)

OpenSSL Improper Authentication Vulnerability

Mutt 1.5.19, when linked against (1) OpenSSL (mutt\_ssl.c) or (2) GnuTLS (mutt\_ssl\_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2009-1390](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1390)

OpenSSL Resource Management Errors Vulnerability

Memory leak in the zlib\_stateful\_finish function in crypto/comp/c\_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO\_cleanup\_all\_ex\_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to [CVE-2008-1678](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1678).

Affected Versions

0.9.2b to 0.9.8k

External References

[CVE-2009-4355](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4355)

OpenSSL Improper Input Validation Vulnerability

OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP\_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

Affected Versions

0.9.2b to 0.9.8h

External References

[CVE-2008-5077](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5077)

OpenSSL Numeric Errors Vulnerability

Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary code via unspecified vectors.

Affected Versions

0.9.8 to 0.9.8e

External References

[CVE-2007-4995](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4995)

OpenSSL Numeric Errors Vulnerability

Off-by-one error in the SSL\_get\_shared\_ciphers function in OpenSSL 0.9.7 up to 0.9.7l, and 0.9.8 up to 0.9.8f, might allow remote attackers to execute arbitrary code via a crafted packet that triggers a one-byte buffer underflow. NOTE: this issue was introduced as a result of a fix for [CVE-2006-3738](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3738). As of 20071012, it is unknown whether code execution is possible.

Affected Versions

0.9.8 to 0.9.8f

External References

[CVE-2007-5135](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5135)

OpenSSL Other Vulnerability

The BN\_from\_montgomery function in crypto/bn/bn\_mont.c in OpenSSL 0.9.8e and earlier does not properly perform Montgomery multiplication, which might allow local users to conduct a side-channel attack and retrieve RSA private keys.

Affected Versions

0.9.2b to 0.9.8e

External References

[CVE-2007-3108](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3108)

OpenSSL Cryptographic Issues Vulnerability

The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms\_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

Affected Versions

0.9.2b to 0.9.8m

External References

[CVE-2010-0742](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0742)

OpenSSL Resource Management Errors Vulnerability

The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

Affected Versions

0.9.2b to 0.9.8s

External References

[CVE-2012-0027](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0027)

OpenSSL Resource Management Errors Vulnerability

The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2012-0027](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0027)

OpenSSL Resource Management Errors Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Versions

0.9.4 to 0.9.8q

External References

[CVE-2011-4619](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4619)

OpenSSL Resource Management Errors Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2011-4619](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4619)

OpenSSL Resource Management Errors Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Versions

0.9.4 to 0.9.8q

External References

[CVE-2011-4577](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4577)

OpenSSL Resource Management Errors Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Versions

0.9.2b to 0.9.8r

External References

[CVE-2011-4577](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4577)

OpenSSL Resource Management Errors Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

Affected Versions

0.9.2b to 0.9.8r

External References

[CVE-2011-4619](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4619)

OpenSSL Cryptographic Issues Vulnerability

crypto/bn/bn\_nist.c in OpenSSL before 0.9.8h on 32-bit platforms, as used in stunnel and other products, in certain circumstances involving ECDH or ECDHE cipher suites, uses an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves, which allows remote attackers to obtain the private key of a TLS server via multiple handshake attempts.

Affected Versions

0.9.2b to 0.9.8f

External References

[CVE-2011-4354](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4354)

OpenSSL Other Vulnerability

The mime\_hdr\_cmp function in crypto/asn1/asn\_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.

Affected Versions

0.9.2b to 0.9.8t

External References

[CVE-2006-7250](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-7250)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The asn1\_d2i\_read\_bio function in crypto/asn1/a\_d2i\_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

Affected Versions

0.9.2b to 0.9.8t

External References

[CVE-2012-2110](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2110)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The asn1\_d2i\_read\_bio function in crypto/asn1/a\_d2i\_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

Affected Versions

0.9.2b to 0.9.8u

External References

[CVE-2012-2110](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2110)

OpenSSL Resource Management Errors Vulnerability

The mime\_param\_cmp function in crypto/asn1/asn\_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than [CVE-2006-7250](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-7250).

Affected Versions

0.9.2b to 0.9.8s

External References

[CVE-2012-1165](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1165)

OpenSSL Resource Management Errors Vulnerability

The mime\_param\_cmp function in crypto/asn1/asn\_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than [CVE-2006-7250](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-7250).

Affected Versions

0.9.2b to 0.9.8t

External References

[CVE-2012-1165](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1165)

OpenSSL Cryptographic Issues Vulnerability

The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

Affected Versions

0.9.2b to 0.9.8s

External References

[CVE-2012-0884](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0884)

OpenSSL Cryptographic Issues Vulnerability

The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

Affected Versions

0.9.2b to 0.9.8t

External References

[CVE-2012-0884](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0884)

OpenSSL Other Vulnerability

The mime\_hdr\_cmp function in crypto/asn1/asn\_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.

Affected Versions

0.9.2b to 0.9.8s

External References

[CVE-2006-7250](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-7250)

OpenSSL Resource Management Errors Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2011-4577](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4577)

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8j, when SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than [CVE-2010-4180](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4180).

Affected Versions

0.9.2b to 0.9.8h

External References

[CVE-2008-7270](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7270)

OpenSSL Cryptographic Issues Vulnerability

OpenSSL before 0.9.8j, when SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than [CVE-2010-4180](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4180).

Affected Versions

0.9.2b to 0.9.8i

External References

[CVE-2008-7270](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7270)

OpenSSL Improper Authentication Vulnerability

OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

Affected Versions

0.9.2b to 0.9.8p

External References

[CVE-2010-4252](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4252)

OpenSSL Improper Authentication Vulnerability

OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2010-4252](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4252)

OpenSSL Other Vulnerability

OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

Affected Versions

0.9.2b to 0.9.8o

External References

[CVE-2010-4180](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4180)

OpenSSL Other Vulnerability

OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

Affected Versions

0.9.2b to 0.9.8p

External References

[CVE-2010-4180](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4180)

OpenSSL Cryptographic Issues Vulnerability

The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE\_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2011-1945](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1945)

OpenSSL Cryptographic Issues Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Versions

0.9.4 to 0.9.8q

External References

[CVE-2011-4576](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4576)

OpenSSL Cryptographic Issues Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Versions

0.9.2b to 0.9.8r

External References

[CVE-2011-4576](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4576)

OpenSSL Cryptographic Issues Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2011-4576](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4576)

OpenSSL Resource Management Errors Vulnerability

Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509\_V\_FLAG\_POLICY\_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.

Affected Versions

0.9.8 to 0.9.8r

External References

[CVE-2011-4109](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4109)

OpenSSL Cryptographic Issues Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Versions

0.9.4 to 0.9.8q

External References

[CVE-2011-4108](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4108)

OpenSSL Cryptographic Issues Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Versions

0.9.2b to 0.9.8r

External References

[CVE-2011-4108](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4108)

OpenSSL Cryptographic Issues Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2011-4108](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4108)

OpenSSL Resource Management Errors Vulnerability

The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.

Affected Versions

0.9.8 to 0.9.8s

External References

[CVE-2011-3210](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3210)

OpenSSL Cryptographic Issues Vulnerability

The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE\_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.

Affected Versions

0.9.2b to 0.9.8p

External References

[CVE-2011-1945](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1945)

OpenSSL Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the ssl3\_get\_new\_session\_ticket function in ssl/s3\_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

Affected Versions

0.9.2b to 0.9.8zf

External References

[CVE-2015-1791](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1791)

OpenSSL Other Vulnerability

The PKCS7\_dataDecodefunction in crypto/pkcs7/pk7\_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

Affected Versions

0.9.2b to 0.9.8zf

External References

[CVE-2015-1790](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1790)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The X509\_cmp\_time function in crypto/x509/x509\_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1\_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

Affected Versions

0.9.2b to 0.9.8zf

External References

[CVE-2015-1789](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1789)

OpenSSL Resource Management Errors Vulnerability

The BN\_GF2m\_mod\_inv function in crypto/bn/bn\_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.

Affected Versions

0.9.2b to 0.9.8zf

External References

[CVE-2015-1788](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1788)

OpenSSL Resource Management Errors Vulnerability

The do\_free\_upto function in crypto/cms/cms\_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

Affected Versions

0.9.2b to 0.9.8zf

External References

[CVE-2015-1792](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1792)

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The ASN1\_TFLG\_COMBINE implementation in crypto/asn1/tasn\_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509\_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

Affected Versions

0.9.2b to 0.9.8zg

External References

[CVE-2015-3195](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3195)

OpenSSL Cryptographic Issues Vulnerability

OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.

Affected Versions

0.9.8d to 0.9.8g

External References

[CVE-2008-0166](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0166)

OpenSSL Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

Internally libssl in OpenSSL calls X509\_verify\_cert() on the client side to verify a certificate supplied by a server. That function may return a negative return value to indicate an internal error (for example out of memory). Such a negative return value is mishandled by OpenSSL and will cause an IO function (such as SSL\_connect() or SSL\_do\_handshake()) to not indicate success and a subsequent call to SSL\_get\_error() to return the value SSL\_ERROR\_WANT\_RETRY\_VERIFY. This return value is only supposed to be returned by OpenSSL if the application has previously called SSL\_CTX\_set\_cert\_verify\_callback(). Since most applications do not do this the SSL\_ERROR\_WANT\_RETRY\_VERIFY return value from SSL\_get\_error() will be totally unexpected and applications may not behave correctly as a result. The exact behaviour will depend on the application but it could result in crashes, infinite loops or other similar incorrect responses. This issue is made more serious in combination with a separate bug in OpenSSL 3.0 that will cause X509\_verify\_cert() to indicate an internal error when processing a certificate chain. This will occur where a certificate does not include the Subject Alternative Name extension but where a Certificate Authority has enforced name constraints. This issue can occur even with valid chains. By combining the two issues an attacker could induce incorrect, application dependent behaviour. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2021-4044](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4044)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

Affected Versions

0.9.7j to 0.9.8zc

External References

[CVE-2017-3735](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3735)

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The get\_client\_master\_key function in s2\_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to [CVE-2016-0800](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800).

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2016-0703](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0703)

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

An oracle protection mechanism in the get\_client\_master\_key function in s2\_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to [CVE-2016-0800](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800).

Affected Versions

0.9.2b to 0.9.8ze

External References

[CVE-2016-0704](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0704)

OpenSSL Numeric Errors Vulnerability

Integer overflow in the EVP\_EncryptUpdate function in crypto/evp/evp\_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2016-2106](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2106)

OpenSSL Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for [CVE-2013-0169](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0169).

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2016-2107](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2107)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2016-2108](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2108)

OpenSSL Resource Management Errors Vulnerability

The asn1\_d2i\_read\_bio function in crypto/asn1/a\_d2i\_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2016-2109](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2109)

OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The X509\_NAME\_oneline function in crypto/x509/x509\_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

Affected Versions

0.9.2b to 0.9.8zh

External References

[CVE-2016-2176](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2176)

OpenSSL Key Management Errors Vulnerability

A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.

Affected Versions

0.9.2b to 0.9.8zh

External References