Open Source Vulnerability Report

BLACKDUCK

C Demo Project>3.4

Phase: DEVELOPMENT | Distribution: EXTERNAL

Vulnerability Status Filter: All Vulnerabilities

69 HIGH	133 MEDIUM	11 LOW

VULNERABLE COMPONENTS SUMMARY

BlueZ 5.23	0	10	0
Condor 7.6.10	1	0	1
GNU C Library 2.22	9	11	2
GnuWin32 1.2.37	36	34	0
OpenSSL 1.0.1d	20	76	8

VULNERABLE COMPONENTS DETAILS

BlueZ 5.23

GNU Lesser General Public License v2.1 or later (weak reciprocal)
GNU General Public License v2.0 or later (reciprocal)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2016-9797	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a buffer over-read was observed in "l2cap_dump" function in "tools/parser/l2cap.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.						
CVE-2016-9798	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a use-after-free was identified in "conf_opt" function in "tools/parser/l2cap.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.						
CVE-2016-9799	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a buffer overflow was observed in "pklg_read_hci" function in "btsnoop.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.						
CVE-2016-9800	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a buffer overflow was observed in "pin_code_reply_dump" function in "tools/parser/hci.c" source file. The issue exists because "pin" array is overflowed by supplied parameter due to lack of boundary checks on size of the buffer from frame "pin_code_reply_cp *cp" parameter.						
CVE-2016-9801	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a buffer overflow was observed in "set_ext_ctrl" function in "tools/parser/l2cap.c" source file when processing corrupted dump file.						
CVE-2016-9802	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a buffer over-read was identified in "l2cap_packet" function in "monitor/packet.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.						
CVE-2016-9803	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, an out-of-bounds read was observed in "le_meta_ev_dump" function in "tools/parser/hci.c" source file. This issue exists because 'subevent' (which is used to read correct element from 'ev_le_meta_str' array) is overflowed.						
CVE-2016-9804	MEDIUM	5.0	2.9	10.0	NEW	12/07/2016
In BlueZ 5.42, a buffer overflow was observed in "commands_dump" function in "tools/parser/csr.c" source file. The issue exists because "commands" array is overflowed by supplied parameter due to lack of boundary checks on size of the buffer from frame "frm->ptr" parameter. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.						
CVE-2016-9917	MEDIUM	5.0	2.9	10.0	NEW	12/23/2016

<table>
<tr><td colspan="7">In BlueZ 5.42, a buffer overflow was observed in "read_n" function in "tools/hcidump.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.</td></tr>
<tr><td>CVE-2016-9918</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>12/23/2016</td></tr>
<tr><td colspan="7">In BlueZ 5.42, an out-of-bounds read was identified in "packet_hexdump" function in "monitor/packet.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.</td></tr>
</table>

Condor 7.6.10

Apache License 2.0 (permissive)

<table>
<tr><th>Vulnerability Name</th><th>Severity</th><th>Base</th><th>Exploitability</th><th>Impact</th><th>Status</th><th>Published</th></tr>
<tr><td>CVE-2012-3416</td><td>HIGH</td><td>10.0</td><td>10.0</td><td>10.0</td><td>NEW</td><td>10/03/2012</td></tr>
<tr><td colspan="7">Condor before 7.8.2 allows remote attackers to bypass host-based authentication and execute actions such as ALLOW_ADMINISTRATOR or ALLOW_WRITE by connecting from a system with a spoofed reverse DNS hostname.</td></tr>
<tr><td>CVE-2013-4255</td><td>LOW</td><td>3.5</td><td>2.9</td><td>6.8</td><td>NEW</td><td>10/15/2013</td></tr>
<tr><td colspan="7">The policy definition evaluator in Condor 7.5.4, 8.0.0, and earlier does not properly handle attributes in a (1) PREEMPT, (2) SUSPEND, (3) CONTINUE, (4) WANT_VACATE, or (5) KILL policy that evaluate to an Unconfigured, Undefined, or Error state, which allows remote authenticated users to cause a denial of service (condor_startd exit) via a crafted job.</td></tr>
</table>

GNU C Library 2.22

GNU Lesser General Public License v2.1 or later (weak reciprocal)
GNU General Public License v2.0 or later (reciprocal)

<table>
<tr><th>Vulnerability Name</th><th>Severity</th><th>Base</th><th>Exploitability</th><th>Impact</th><th>Status</th><th>Published</th></tr>
<tr><td>133568</td><td>MEDIUM</td><td>6.4</td><td>4.9</td><td>10.0</td><td>DUPLICATE</td><td>05/17/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains an out-of-bounds read flaw in the strftime() function that is triggered when handling time values. This may allow a context-dependent attacker to crash a process linked against the library or potentially disclose memory contents.</td></tr>
<tr><td>133572</td><td>LOW</td><td>2.1</td><td>2.9</td><td>3.9</td><td>DUPLICATE</td><td>12/09/2016</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains a flaw that is triggered as LD_POINTER_GUARD is not properly handled in some circumstances. This may potentially allow a local attacker to bypass security restrictions.</td></tr>
<tr><td>133574</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>DUPLICATE</td><td>05/17/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains an integer overflow flaw that is triggered as hcreate and hcreate_r do not properly fail when handling large element counts. This may allow a context-dependent attacker to cause an out-of-bounds write that will allow the attacker to execute arbitrary code.</td></tr>
<tr><td>133577</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>DUPLICATE</td><td>05/17/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains an overflow condition in the catopen() function. The issue is triggered as user-supplied input is not properly validated when handling strings. This may allow a context-dependent attacker to cause a stack-based buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code.</td></tr>
<tr><td>133580</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>DUPLICATE</td><td>05/17/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains an overflow condition in multiple nan functions, such as nanf() and nanl(). The issue is triggered as user-supplied input is not properly validated when handling a crafted string. This may allow a context-dependent attacker to cause a stack-based buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code.</td></tr>
<tr><td>134584</td><td>HIGH</td><td>9.3</td><td>10.0</td><td>8.6</td><td>DUPLICATE</td><td>02/15/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains an overflow condition in the send_dg() and send_vc() functions in libresolv resolv/res_send.c. The issue is triggered as user-supplied input is not properly validated when looking up domain names via the getaddrinfo() call. This may allow a remote attacker to cause a stack-based buffer overflow, resulting in a denial of service or potentially allowing the execution of arbitrary code.</td></tr>
<tr><td>142436</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>04/20/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains a flaw in the name resolution function call handling. The issue is triggered when initializing a partial internal resolver data structure. With a specially crafted request, an attacker can cause a memory leak. It is not immediately clear is this is a memory information disclosure or a memory leak leading to a denial of service.</td></tr>
<tr><td>152759</td><td>HIGH</td><td>7.1</td><td>6.9</td><td>8.6</td><td>NEW</td><td>03/01/2017</td></tr>
</table>

<table>
<tr><td colspan="7">GNU C Library (glibc) contains a flaw that is triggered during the handling of specially crafted multi-byte sequences. This may allow a context-dependent attacker to trigger an infinite loop and cause a process linked against the library to hang.</td></tr>
<tr><td>98836</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>04/20/2017</td></tr>
<tr><td colspan="7">GNU C Library (glibc) contains an overflow condition in the gethosts function in sysdeps/posix/getaddrinfo.c. The issue is triggered as user-supplied input is not properly validated during the handling of domain conversion results. This may allow a remote attacker to cause a stack-based buffer overflow, crashing a process linked against the library.</td></tr>
<tr><td>CVE-2014-9761</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>11/28/2016</td></tr>
<tr><td colspan="7">Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.</td></tr>
<tr><td>CVE-2015-7547</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>NEW</td><td>02/16/2017</td></tr>
<tr><td colspan="7">Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.</td></tr>
<tr><td>CVE-2015-8776</td><td>MEDIUM</td><td>6.4</td><td>4.9</td><td>10.0</td><td>NEW</td><td>12/02/2016</td></tr>
<tr><td colspan="7">The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.</td></tr>
<tr><td>CVE-2015-8777</td><td>LOW</td><td>2.1</td><td>2.9</td><td>3.9</td><td>NEW</td><td>12/05/2016</td></tr>
<tr><td colspan="7">The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.</td></tr>
<tr><td>CVE-2015-8778</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>12/02/2016</td></tr>
<tr><td colspan="7">Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.</td></tr>
<tr><td>CVE-2015-8779</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>12/02/2016</td></tr>
<tr><td colspan="7">Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.</td></tr>
<tr><td>CVE-2016-10228</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>03/03/2017</td></tr>
<tr><td colspan="7">The iconv program in the GNU C Library (aka glibc or libc6) 2.25 and earlier, when invoked with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.</td></tr>
<tr><td>CVE-2016-1234</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>11/28/2016</td></tr>
<tr><td colspan="7">Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.</td></tr>
<tr><td>CVE-2016-3075</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>11/28/2016</td></tr>
<tr><td colspan="7">Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name.</td></tr>
<tr><td>CVE-2016-3706</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>02/01/2017</td></tr>
<tr><td colspan="7">Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (aka glibc or libc6) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4458.</td></tr>
<tr><td>CVE-2016-4429</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>02/01/2017</td></tr>
<tr><td colspan="7">Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.</td></tr>
<tr><td>CVE-2016-5417</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>02/17/2017</td></tr>
<tr><td colspan="7">Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or</td></tr>
</table>

libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.						
CVE-2016-6323	MEDIUM	5.0	2.9	10.0	NEW	02/01/2017
The makecontext function in the GNU C Library (aka glibc or libc6) before 2.25 creates execution contexts incompatible with the unwinder on ARM EABI (32-bit) platforms, which might allow context-dependent attackers to cause a denial of service (hang), as demonstrated by applications compiled using gccgo, related to backtrace generation.						

GnuWin32 1.2.37

GnuWin32 - Libarchive License (BSD -) (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2007-2754	MEDIUM	6.8	6.4	8.6	NEW	10/30/2012
Integer signedness error in truetype/ttgload.c in Freetype 2.3.4 and earlier might allow remote attackers to execute arbitrary code via a crafted TTF image with a negative n_points value, which leads to an integer overflow and heap-based buffer overflow.						
CVE-2007-3506	HIGH	7.5	6.4	10.0	NEW	09/05/2008
The ft_bitmap_assure_buffer function in src/base/ftbimap.c in FreeType 2.3.3 allows context-dependent attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors involving bitmap fonts, related to a "memory buffer overwrite bug."						
CVE-2009-0946	HIGH	10.0	10.0	10.0	NEW	11/18/2010
Multiple integer overflows in FreeType 2.3.9 and earlier allow remote attackers to execute arbitrary code via vectors related to large values in certain inputs in (1) smooth/ftsmooth.c, (2) sfnt/ttcmap.c, and (3) cff/cffload.c.						
CVE-2009-2624	MEDIUM	6.8	6.4	8.6	NEW	11/18/2010
The huft_build function in inflate.c in gzip before 1.3.13 creates a hufts (aka huffman) table that is too small, which allows remote attackers to cause a denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive. NOTE: this issue is caused by a CVE-2006-4334 regression.						
CVE-2010-2497	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Integer underflow in glyph handling in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2498	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
The psh_glyph_find_strong_points function in pshinter/pshalgo.c in FreeType before 2.4.0 does not properly implement hinting masks, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted font file that triggers an invalid free operation.						
CVE-2010-2499	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted LaserWriter PS font file with an embedded PFB fragment.						
CVE-2010-2500	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Integer overflow in the gray_render_span function in smooth/ftgrays.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2519	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Heap-based buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted length value in a POST fragment header in a font file.						
CVE-2010-2520	MEDIUM	5.1	6.4	4.9	NEW	12/18/2012
Heap-based buffer overflow in the Ins_IUP function in truetype/ttinterp.c in FreeType before 2.4.0, when TrueType bytecode support is enabled, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2527	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Multiple buffer overflows in demo programs in FreeType before 2.4.0 allow remote attackers to cause a denial of service						

(application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2541	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Buffer overflow in ftmulti.c in the ftmulti demo program in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2805	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
The FT_Stream_EnterFrame function in base/ftstream.c in FreeType before 2.4.2 does not properly validate certain position values, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2806	MEDIUM	6.8	6.4	8.6	NEW	01/12/2011
Array index error in the t42_parse_sfnts function in type42/t42parse.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via negative size values for certain strings in FontType42 font files, leading to a heap-based buffer overflow.						
CVE-2010-2807	MEDIUM	6.8	6.4	8.6	NEW	12/10/2010
FreeType before 2.4.2 uses incorrect integer data types during bounds checking, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.						
CVE-2010-2808	MEDIUM	6.8	6.4	8.6	NEW	01/12/2011
Buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted Adobe Type 1 Mac Font File (aka LWFN) font.						
CVE-2010-3053	MEDIUM	4.3	2.9	8.6	NEW	12/18/2012
bdf/bdflib.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) via a crafted BDF font file, related to an attempted modification of a value in a static string.						
CVE-2010-3311	HIGH	9.3	10.0	8.6	NEW	12/18/2012
Integer overflow in base/ftstream.c in libXft (aka the X FreeType library) in FreeType before 2.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted Compact Font Format (CFF) font file that triggers a heap-based buffer overflow, related to an "input stream position error" issue, a different vulnerability than CVE-2010-1797.						
CVE-2010-3814	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Heap-based buffer overflow in the Ins_SHZ function in ttinterp.c in FreeType 2.4.3 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted SHZ bytecode instruction, related to TrueType opcodes, as demonstrated by a PDF document with a crafted embedded font.						
CVE-2010-3855	MEDIUM	6.8	6.4	8.6	NEW	12/18/2012
Buffer overflow in the ft_var_readpackedpoints function in truetype/ttgxvar.c in FreeType 2.4.3 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted TrueType GX font.						
CVE-2011-0226	HIGH	9.3	10.0	8.6	NEW	10/25/2011
Integer signedness error in psaux/t1decode.c in FreeType before 2.4.6, as used in CoreGraphics in Apple iOS before 4.2.9 and 4.3.x before 4.3.4 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Type 1 font in a PDF document, as exploited in the wild in July 2011.						
CVE-2012-1126	HIGH	10.0	10.0	10.0	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted property data in a BDF font.						
CVE-2012-1127	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted glyph or bitmap data in a BDF font.						
CVE-2012-1128	HIGH	9.3	10.0	8.6	NEW	12/18/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a						

denial of service (NULL pointer dereference and memory corruption) or possibly execute arbitrary code via a crafted TrueType font.						
CVE-2012-1129	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted SFNT string in a Type 42 font.						
CVE-2012-1130	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted property data in a PCF font.						
CVE-2012-1131	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, on 64-bit platforms allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via vectors related to the cell table of a font.						
CVE-2012-1132	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted dictionary data in a Type 1 font.						
CVE-2012-1133	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted glyph or bitmap data in a BDF font.						
CVE-2012-1134	HIGH	9.3	10.0	8.6	NEW	07/14/2013
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted private-dictionary data in a Type 1 font.						
CVE-2012-1135	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via vectors involving the NPUSHB and NPUSHW instructions in a TrueType font.						
CVE-2012-1136	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted glyph or bitmap data in a BDF font that lacks an ENCODING field.						
CVE-2012-1137	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted header in a BDF font.						
CVE-2012-1138	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via vectors involving the MIRP instruction in a TrueType font.						
CVE-2012-1139	HIGH	9.3	10.0	8.6	NEW	12/28/2012
Array index error in FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid stack read operation and memory corruption) or possibly execute arbitrary code via crafted glyph data in a BDF font.						
CVE-2012-1140	HIGH	9.3	10.0	8.6	NEW	12/18/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted PostScript						

font object.						
CVE-2012-1141	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted ASCII string in a BDF font.						
CVE-2012-1142	HIGH	9.3	10.0	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted glyph-outline data in a font.						
CVE-2012-1143	MEDIUM	4.3	2.9	8.6	NEW	12/28/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted font.						
CVE-2012-1144	HIGH	9.3	10.0	8.6	NEW	12/18/2012
FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via a crafted TrueType font.						
CVE-2012-5668	MEDIUM	4.3	2.9	8.6	NEW	12/06/2016
FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to BDF fonts and the improper handling of an "allocation error" in the bdf_free_font function.						
CVE-2012-5669	MEDIUM	4.3	2.9	8.6	NEW	12/06/2016
The _bdf_parse_glyphs function in FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to BDF fonts and an incorrect calculation that triggers an out-of-bounds read.						
CVE-2012-5670	MEDIUM	4.3	2.9	8.6	NEW	12/06/2016
The _bdf_parse_glyphs function in FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) via vectors related to BDF fonts and an ENCODING field with a negative value.						
CVE-2014-2240	HIGH	7.5	6.4	10.0	NEW	04/01/2014
Stack-based buffer overflow in the cf2_hintmap_build function in cff/cf2hints.c in FreeType before 2.5.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large number of stem hints in a font file.						
CVE-2014-2241	MEDIUM	6.8	6.4	8.6	NEW	04/01/2014
The (1) cf2_initLocalRegionBuffer and (2) cf2_initGlobalRegionBuffer functions in cff/cf2ft.c in FreeType before 2.5.3 do not properly check if a subroutine exists, which allows remote attackers to cause a denial of service (assertion failure), as demonstrated by a crafted ttf file.						
CVE-2014-9656	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The tt_sbit_decoder_load_image function in sfnt/ttsbit.c in FreeType before 2.5.4 does not properly check for an integer overflow, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted OpenType font.						
CVE-2014-9657	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The tt_face_load_hdmx function in truetype/ttpload.c in FreeType before 2.5.4 does not establish a minimum record size, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted TrueType font.						
CVE-2014-9658	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The tt_face_load_kern function in sfnt/ttkern.c in FreeType before 2.5.4 enforces an incorrect minimum table length, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted TrueType font.						
CVE-2014-9659	HIGH	7.5	6.4	10.0	NEW	11/22/2016
cff/cf2intrp.c in the CFF CharString interpreter in FreeType before 2.5.4 proceeds with additional hints after the hint mask has been computed, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer						

overflow) via a crafted OpenType font. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-2240.

CVE-2014-9660	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The _bdf_parse_glyphs function in bdf/bdflib.c in FreeType before 2.5.4 does not properly handle a missing ENDCHAR record, which allows remote attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a crafted BDF font.						
CVE-2014-9661	HIGH	7.5	6.4	10.0	NEW	01/02/2017
type42/t42parse.c in FreeType before 2.5.4 does not consider that scanning can be incomplete without triggering an error, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted Type42 font.						
CVE-2014-9662	HIGH	7.5	6.4	10.0	NEW	01/02/2017
cff/cf2ft.c in FreeType before 2.5.4 does not validate the return values of point-allocation functions, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted OTF font.						
CVE-2014-9663	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The tt_cmap4_validate function in sfnt/ttcmap.c in FreeType before 2.5.4 validates a certain length field before that field's value is completely calculated, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted cmap SFNT table.						
CVE-2014-9664	MEDIUM	6.8	6.4	8.6	NEW	01/02/2017
FreeType before 2.5.4 does not check for the end of the data during certain parsing actions, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted Type42 font, related to type42/t42parse.c and type1/t1load.c.						
CVE-2014-9665	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The Load_SBit_Png function in sfnt/pngshim.c in FreeType before 2.5.4 does not restrict the rows and pitch values of PNG data, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact by embedding a PNG file in a .ttf font file.						
CVE-2014-9666	MEDIUM	6.8	6.4	8.6	NEW	01/02/2017
The tt_sbit_decoder_init function in sfnt/ttsbit.c in FreeType before 2.5.4 proceeds with a count-to-size association without restricting the count value, which allows remote attackers to cause a denial of service (integer overflow and out-of-bounds read) or possibly have unspecified other impact via a crafted embedded bitmap.						
CVE-2014-9667	MEDIUM	6.8	6.4	8.6	NEW	01/02/2017
sfnt/ttload.c in FreeType before 2.5.4 proceeds with offset+length calculations without restricting the values, which allows remote attackers to cause a denial of service (integer overflow and out-of-bounds read) or possibly have unspecified other impact via a crafted SFNT table.						
CVE-2014-9668	HIGH	7.5	6.4	10.0	NEW	01/02/2017
The woff_open_font function in sfnt/sfobjs.c in FreeType before 2.5.4 proceeds with offset+length calculations without restricting length values, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact via a crafted Web Open Font Format (WOFF) file.						
CVE-2014-9669	MEDIUM	6.8	6.4	8.6	NEW	01/02/2017
Multiple integer overflows in sfnt/ttcmap.c in FreeType before 2.5.4 allow remote attackers to cause a denial of service (out-of-bounds read or memory corruption) or possibly have unspecified other impact via a crafted cmap SFNT table.						
CVE-2014-9670	MEDIUM	4.3	2.9	8.6	NEW	01/02/2017
Multiple integer signedness errors in the pcf_get_encodings function in pcf/pcfread.c in FreeType before 2.5.4 allow remote attackers to cause a denial of service (integer overflow, NULL pointer dereference, and application crash) via a crafted PCF file that specifies negative values for the first column and first row.						
CVE-2014-9671	MEDIUM	4.3	2.9	8.6	NEW	01/02/2017
Off-by-one error in the pcf_get_properties function in pcf/pcfread.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PCF file with a 0xffffffff size value that is improperly incremented.						
CVE-2014-9672	MEDIUM	5.8	4.9	8.6	NEW	01/02/2017

<table>
<tr><td colspan="7">Array index error in the parse_fond function in base/ftmac.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (out-of-bounds read) or obtain sensitive information from process memory via a crafted FOND resource in a Mac font file.</td></tr>
<tr><td>CVE-2014-9673</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>NEW</td><td>01/02/2017</td></tr>
<tr><td colspan="7">Integer signedness error in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted Mac font.</td></tr>
<tr><td>CVE-2014-9674</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>01/02/2017</td></tr>
<tr><td colspan="7">The Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 proceeds with adding to length values without validating the original values, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact via a crafted Mac font.</td></tr>
<tr><td>CVE-2014-9675</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>01/02/2017</td></tr>
<tr><td colspan="7">bdf/bdflib.c in FreeType before 2.5.4 identifies property names by only verifying that an initial substring is present, which allows remote attackers to discover heap pointer values and bypass the ASLR protection mechanism via a crafted BDF font.</td></tr>
<tr><td>CVE-2014-9745</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>12/07/2016</td></tr>
<tr><td colspan="7">The parse_encoding function in type1/t1load.c in FreeType before 2.5.3 allows remote attackers to cause a denial of service (infinite loop) via a "broken number-with-base" in a Postscript stream, as demonstrated by 8#garbage.</td></tr>
<tr><td>CVE-2014-9746</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>06/07/2016</td></tr>
<tr><td colspan="7">The (1) t1_parse_font_matrix function in type1/t1load.c, (2) cid_parse_font_matrix function in cid/cidload.c, (3) t42_parse_font_matrix function in type42/t42parse.c, and (4) ps_parser_load_field function in psaux/psobjs.c in FreeType before 2.5.4 do not check return values, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted font.</td></tr>
<tr><td>CVE-2014-9747</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>06/08/2016</td></tr>
<tr><td colspan="7">The t42_parse_encoding function in type42/t42parse.c in FreeType before 2.5.4 does not properly update the current position for immediates-only mode, which allows remote attackers to cause a denial of service (infinite loop) via a Type42 font.</td></tr>
<tr><td>CVE-2016-10244</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>NEW</td><td>04/07/2017</td></tr>
<tr><td colspan="7">The parse_charstrings function in type1/t1load.c in FreeType 2 before 2.7 does not ensure that a font contains a glyph name, which allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted file.</td></tr>
<tr><td>CVE-2017-8105</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>04/28/2017</td></tr>
<tr><td colspan="7">FreeType 2 before 2017-03-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_decoder_parse_charstrings function in psaux/t1decode.c.</td></tr>
</table>

OpenSSL 1.0.1d

SSLeay License (weak reciprocal)
OpenSSL Combined License (permissive)

<table>
<tr><th>Vulnerability Name</th><th>Severity</th><th>Base</th><th>Exploitability</th><th>Impact</th><th>Status</th><th>Published</th></tr>
<tr><td>101347</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>DUPLICATE</td><td>11/02/2016</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw in the ssl_get_algorithm2() function in ssl/s3_lib.c that is triggered when determining the TLS version and which hash to use during the handling of specially crafted traffic. This may allow a remote attacker to crash an application linked against the library.</td></tr>
<tr><td>101597</td><td>MEDIUM</td><td>5.4</td><td>6.9</td><td>4.9</td><td>DUPLICATE</td><td>08/25/2016</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw in the DTLS (Datagram Transport Layer Security) protocol implementation that is triggered when a handshake renegotiation packet is lost or discarded. This may allow an attacker capable of intercepting communication between a client and server (i.e. Man-in-the-Middle) to crash the DTLS client or server application.</td></tr>
<tr><td>101843</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>DUPLICATE</td><td>12/12/2016</td></tr>
<tr><td colspan="7">OpenSSL contains a NULL pointer dereference flaw in the ssl3_take_mac() function in ssl/s3_both.c that is triggered when handling handshakes with tampered TLS records. With a specially crafted request, a remote attacker can cause a service to crash.</td></tr>
<tr><td>104810</td><td>LOW</td><td>1.9</td><td>2.9</td><td>3.4</td><td>DUPLICATE</td><td>05/10/2017</td></tr>
</table>

<table>
<tr><td colspan="6">OpenSSL contains a flaw in the ECDSA (Elliptic Curve Digital Signature Algorithm) implementation that is triggered when subject to a so-called FLUSH+RELOAD cache side-channel attack. This may allow a malicious process to recover ECDSA nonces.</td></tr>
<tr><td>105465</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>DUPLICATE</td><td>03/09/2017</td></tr>
<tr><td colspan="7">OpenSSL contains an out-of-bounds read flaw in the dtls1_process_heartbeat() function in ssl/d1_both.c and tls1_process_heartbeat() function in ssl/t1_lib.c. The issue is triggered during the handling of TLS heartbeat extensions. This allows a remote attacker to disclose up to 64k of memory at a time, which may contain sensitive information including secret keys, which would allow decryption of all traffic to and from the server. This will affect any service that uses TLS and is not limited to HTTPS. This includes SMTP servers that support STARTTLS as well as IMAPS. Additionally, both servers and clients are affected.</td></tr>
<tr><td>107729</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>DUPLICATE</td><td>05/10/2017</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw in the handshake process. With a carefully crafted handshake, a remote attacker can force the client or server to use weak keying material. This can then be leveraged to conduct a Man-in-the-Middle (MitM) attack allowing for the decryption or modification of traffic between the victim client and server.</td></tr>
<tr><td>113373</td><td>HIGH</td><td>7.1</td><td>6.9</td><td>8.6</td><td>DUPLICATE</td><td>12/13/2016</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw in the DTLS SRTP extension parsing code that is triggered when handling a specially crafted handshake message, which can cause a memory leak. This may allow a remote attacker to cause a denial of service.</td></tr>
<tr><td>113374</td><td>HIGH</td><td>7.1</td><td>6.9</td><td>8.6</td><td>DUPLICATE</td><td>12/13/2016</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw in the SSL, TLS, and DTLS servers that is triggered when handling a session ticket that has failed to have its integrity properly verified, which can result in a memory leak. With a large number of invalid session tickets, a remote attacker can cause a denial of service.</td></tr>
<tr><td>113377</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>DUPLICATE</td><td>12/21/2016</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw that is triggered as the 'no-ssl3' build option is not properly honored by the program, which can cause insecure SSL 3.0 handshakes to be accepted and completed.</td></tr>
<tr><td>113829</td><td>LOW</td><td>2.6</td><td>2.9</td><td>4.9</td><td>NEW</td><td>06/25/2016</td></tr>
<tr><td colspan="7">The Secure Sockets Layer (SSL) v3 protocol contains a weak key derivation process that is due to half of the established master key being fully dependent on the MD5 hash function. This may allow attackers to more easily conduct attacks related to hash collisions, which in-turn makes the protocol insecure.</td></tr>
<tr><td>122875</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>DUPLICATE</td><td>02/17/2017</td></tr>
<tr><td colspan="7">OpenSSL contains a race condition in the NewSessionTicket functionality that is triggered when a NewSessionTicket request is received by a multi-threaded client while attempting to re-use a previous ticket. This may allow a remote attacker to cause a double-free and have an unspecified impact.</td></tr>
<tr><td>123172</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>DUPLICATE</td><td>02/07/2017</td></tr>
<tr><td colspan="7">OpenSSL contains an infinite loop condition in the BN_GF2m_mod_inv() function in crypto/bn/bn_gf2m.c. The issue is triggered during the handling of the polynomial field when parsing a ECParameters structure. This may allow a remote attacker to cause an application linked against the library to stop responding and exhaust available system resources.</td></tr>
<tr><td>123173</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>DUPLICATE</td><td>02/07/2017</td></tr>
<tr><td colspan="7">OpenSSL contains an out-of-bounds read flaw in the X509_cmp_time() function in crypto/x509/x509_vfy.c that is triggered as the length of ASN1_TIME strings is not properly checked. With a specially crafted certificate or CRL, a remote attacker can crash an application linked against the library or potentially disclose memory contents.</td></tr>
<tr><td>123174</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>DUPLICATE</td><td>02/07/2017</td></tr>
<tr><td colspan="7">OpenSSL contains a NULL pointer dereference flaw in the PKCS7_dataDecode() function in crypto/pkcs7/pk7_doit.c that is triggered when handling ASN.1-encoded PKCS#7 blobs with missing content. This may allow a remote attacker to crash an application linked against the library.</td></tr>
<tr><td>123175</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>DUPLICATE</td><td>02/07/2017</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw that is triggered when handling an unknown hash function OID during the verification of a signedData message, which cause cause the CMS mode to enter an infinite loop. This may allow a remote attacker to cause a denial of service.</td></tr>
<tr><td>123176</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>DUPLICATE</td><td>02/07/2017</td></tr>
<tr><td colspan="7">OpenSSL contains a flaw that is triggered as user-supplied input is not properly validated when a DTLS peer handles application</td></tr>
</table>

data between the ChangeCipherSpec and Finished messages. This may allow a remote attacker to cause an invalid free, which will corrupt memory and cause a denial of service or potentially execute arbitrary code.						
137577	HIGH	7.8	6.9	10.0	DUPLICATE	05/19/2017
OpenSSL contains a flaw in crypto/asn1/a_d2i_fp.c that is triggered during the handling of large length fields in ASN.1 BIO. This may allow a remote attacker to exhaust memory resources, potentially crashing a process linked against the library.						
137896	LOW	2.6	2.9	4.9	DUPLICATE	05/19/2017
OpenSSL contains a flaw in the aesni_cbc_hmac_sha1_cipher() function in crypto/evp/e_aes_cbc_hmac_sha1.c and aesni_cbc_hmac_sha256_cipher() function in crypto/evp/e_aes_cbc_hmac_sha256.c. The issue is triggered when a connection uses an AES CBC cipher and AES-NI is supported by the server. This may allow a MitM (Man-in-the-Middle) attacker to conduct a padding oracle attack to potentially decrypt traffic.						
137897	MEDIUM	6.4	4.9	10.0	DUPLICATE	05/19/2017
OpenSSL contains an out-of-bounds read flaw in the X509_NAME_oneline() function in crypto/x509/x509_obj.c that is triggered when handling overly long ASN1 strings. This may allow a remote attacker to potentially disclose arbitrary stack memory contents.						
137898	MEDIUM	5.0	2.9	10.0	DUPLICATE	05/19/2017
OpenSSL contains an overflow condition in the EVP_EncryptUpdate() function in crypto/evp/evp_enc.c that is triggered when handling a large amount of input data after a previous call to the same function with a partial block. This may allow a context-dependent attacker to cause a heap-based buffer overflow, crashing a process linked against the library or potentially resulting in the execution of arbitrary code.						
137899	MEDIUM	5.0	2.9	10.0	DUPLICATE	05/19/2017
OpenSSL contains an overflow condition in the EVP_EncodeUpdate() function in crypto/evp/encode.c that is triggered when handling a large amount of input data. This may allow a context-dependent attacker to cause a heap-based buffer overflow, crashing a process linked against the library or potentially resulting in the execution of arbitrary code.						
137900	HIGH	10.0	10.0	10.0	DUPLICATE	05/19/2017
OpenSSL contains an underflow condition in the ASN.1 encoder that is triggered when attempting to encode the value zero represented as a negative integer. This may allow a remote attacker to corrupt memory and potentially execute arbitrary code.						
CVE-2010-5298	MEDIUM	4.0	4.9	4.9	NEW	01/26/2017
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.						
CVE-2013-4353	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017
The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.						
CVE-2013-6449	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017
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.						
CVE-2013-6450	MEDIUM	5.8	4.9	8.6	NEW	01/06/2017
The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.						
CVE-2014-0160	MEDIUM	5.0	2.9	10.0	NEW	01/06/2017
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.						
CVE-2014-0195	MEDIUM	6.8	6.4	8.6	NEW	01/06/2017
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.						

<table>
<tr><td>CVE-2014-0198</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>01/18/2017</td></tr>
<tr><td colspan="7">The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.</td></tr>
<tr><td>CVE-2014-0221</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2014-0224</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>NEW</td><td>01/18/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2014-3470</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>01/18/2017</td></tr>
<tr><td colspan="7">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 1.0.1 h, 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.</td></tr>
<tr><td>CVE-2014-3505</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2014-3506</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2014-3507</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2014-3508</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">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 1.0.1 i, 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.</td></tr>
<tr><td>CVE-2014-3509</td><td>MEDIUM</td><td>6.8</td><td>6.4</td><td>8.6</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.</td></tr>
<tr><td>CVE-2014-3510</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2014-3511</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a "protocol downgrade" issue.</td></tr>
<tr><td>CVE-2014-3512</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>01/06/2017</td></tr>
<tr><td colspan="7">Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B</td></tr>
</table>

parameter.						
CVE-2014-3513	HIGH	7.1	6.9	8.6	NEW	01/02/2017
Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.						
CVE-2014-3566	MEDIUM	4.3	2.9	8.6	NEW	03/23/2017
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.						
CVE-2014-3567	HIGH	7.1	6.9	8.6	NEW	01/02/2017
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.						
CVE-2014-3568	MEDIUM	4.3	2.9	8.6	NEW	01/02/2017
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.						
CVE-2014-3570	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2014-3571	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2014-3572	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2014-5139	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017
The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.						
CVE-2014-8176	HIGH	7.5	6.4	10.0	NEW	12/30/2016
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.						
CVE-2014-8275	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2015-0204	MEDIUM	4.3	2.9	8.6	NEW	01/02/2017
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.						
CVE-2015-0205	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers						

to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.						
CVE-2015-0206	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.						
CVE-2015-0207	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
The dtls1_listen function in d1_lib.c in OpenSSL 1.0.2 before 1.0.2a does not properly isolate the state information of independent data streams, which allows remote attackers to cause a denial of service (application crash) via crafted DTLS traffic, as demonstrated by DTLS 1.0 traffic to a DTLS 1.2 server.						
CVE-2015-0208	MEDIUM	4.3	2.9	8.6	NEW	01/02/2017
The ASN.1 signature-verification implementation in the rsa_item_verify function in crypto/rsa/rsa_ameth.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted RSA PSS parameters to an endpoint that uses the certificate-verification feature.						
CVE-2015-0209	MEDIUM	6.8	6.4	8.6	NEW	01/02/2017
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 1.0.0 r, 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.						
CVE-2015-0285	MEDIUM	4.3	2.9	8.6	NEW	01/02/2017
The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before proceeding with a handshake, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and then conducting a brute-force attack.						
CVE-2015-0286	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2015-0287	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2015-0288	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2015-0289	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2015-0290	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
The multi-block feature in the ssl3_write_bytes function in s3_pkt.c in OpenSSL 1.0.2 before 1.0.2a on 64-bit x86 platforms with AES NI support does not properly handle certain non-blocking I/O cases, which allows remote attackers to cause a denial of service (pointer corruption and application crash) via unspecified vectors.						
CVE-2015-0291	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
The sigalgs implementation in t1_lib.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by using an invalid signature_algorithms extension in the ClientHello message during a renegotiation.						
CVE-2015-0292	HIGH	7.5	6.4	10.0	NEW	01/02/2017

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.						
CVE-2015-0293	MEDIUM	5.0	2.9	10.0	NEW	01/02/2017
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.						
CVE-2015-1787	LOW	2.6	2.9	4.9	NEW	01/02/2017
The ssl3_get_client_key_exchange function in s3_srvr.c in OpenSSL 1.0.2 before 1.0.2a, when client authentication and an ephemeral Diffie-Hellman ciphersuite are enabled, allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.						
CVE-2015-1788	MEDIUM	4.3	2.9	8.6	NEW	12/30/2016
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.						
CVE-2015-1789	MEDIUM	4.3	2.9	8.6	NEW	12/30/2016
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.						
CVE-2015-1790	MEDIUM	5.0	2.9	10.0	NEW	12/30/2016
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.						
CVE-2015-1791	MEDIUM	6.8	6.4	8.6	NEW	12/30/2016
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.						
CVE-2015-1792	MEDIUM	5.0	2.9	10.0	NEW	12/30/2016
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.						
CVE-2015-3194	MEDIUM	5.0	2.9	10.0	NEW	05/08/2017
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.						
CVE-2015-3195	MEDIUM	5.0	2.9	10.0	NEW	05/08/2017
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.						
CVE-2015-3196	MEDIUM	4.3	2.9	8.6	NEW	05/08/2017
ssl/s3_clnt.c in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p, and 1.0.2 before 1.0.2d, when used for a multi-threaded client, writes the PSK identity hint to an incorrect data structure, which allows remote servers to cause a denial of service (race condition and double free) via a crafted ServerKeyExchange message.						
CVE-2015-3197	MEDIUM	4.3	2.9	8.6	NEW	05/09/2017
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.						

CVE-2015-4000	MEDIUM	4.3	2.9	8.6	NEW	12/30/2016
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.						
CVE-2016-0702	LOW	1.9	2.9	3.4	NEW	05/09/2017
The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a "CacheBleed" attack.						
CVE-2016-0703	MEDIUM	4.3	2.9	8.6	NEW	05/09/2017
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.						
CVE-2016-0704	MEDIUM	4.3	2.9	8.6	NEW	05/09/2017
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.						
CVE-2016-0705	HIGH	10.0	10.0	10.0	NEW	05/09/2017
Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.						
CVE-2016-0797	MEDIUM	5.0	2.9	10.0	NEW	05/09/2017
Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c.						
CVE-2016-0798	HIGH	7.8	6.9	10.0	NEW	05/09/2017
Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c.						
CVE-2016-0799	HIGH	10.0	10.0	10.0	NEW	05/09/2017
The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.						
CVE-2016-0800	MEDIUM	4.3	2.9	8.6	NEW	05/09/2017
The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.						
CVE-2016-2105	MEDIUM	5.0	2.9	10.0	NEW	02/28/2017
Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.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 binary data.						
CVE-2016-2106	MEDIUM	5.0	2.9	10.0	NEW	02/28/2017
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.						
CVE-2016-2107	LOW	2.6	2.9	4.9	NEW	05/09/2017
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						

<table>
<tr><td colspan="7">an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.</td></tr>
<tr><td>CVE-2016-2108</td><td>HIGH</td><td>10.0</td><td>10.0</td><td>10.0</td><td>NEW</td><td>05/09/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2016-2109</td><td>HIGH</td><td>7.8</td><td>6.9</td><td>10.0</td><td>NEW</td><td>02/28/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2016-2176</td><td>MEDIUM</td><td>6.4</td><td>4.9</td><td>10.0</td><td>NEW</td><td>02/28/2017</td></tr>
<tr><td colspan="7">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.</td></tr>
<tr><td>CVE-2016-2177</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.</td></tr>
<tr><td>CVE-2016-2178</td><td>LOW</td><td>2.1</td><td>2.9</td><td>3.9</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.</td></tr>
<tr><td>CVE-2016-2179</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.</td></tr>
<tr><td>CVE-2016-2180</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.</td></tr>
<tr><td>CVE-2016-2181</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.</td></tr>
<tr><td>CVE-2016-2182</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>03/07/2017</td></tr>
<tr><td colspan="7">The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.</td></tr>
<tr><td>CVE-2016-2183</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>05/09/2017</td></tr>
<tr><td colspan="7">The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.</td></tr>
<tr><td>CVE-2016-2842</td><td>HIGH</td><td>10.0</td><td>10.0</td><td>10.0</td><td>NEW</td><td>05/09/2017</td></tr>
<tr><td colspan="7">The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.</td></tr>
<tr><td>CVE-2016-6302</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.</td></tr>
</table>

<table>
<tr><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td>CVE-2016-6303</td><td>HIGH</td><td>7.5</td><td>6.4</td><td>10.0</td><td>NEW</td><td>02/23/2017</td></tr>
<tr><td colspan="7">Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.</td></tr>
<tr><td>CVE-2016-6304</td><td>HIGH</td><td>7.8</td><td>6.9</td><td>10.0</td><td>NEW</td><td>02/01/2017</td></tr>
<tr><td colspan="7">Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.</td></tr>
<tr><td>CVE-2016-6306</td><td>MEDIUM</td><td>4.3</td><td>2.9</td><td>8.6</td><td>NEW</td><td>02/01/2017</td></tr>
<tr><td colspan="7">The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.</td></tr>
<tr><td>CVE-2016-7055</td><td>LOW</td><td>2.6</td><td>2.9</td><td>4.9</td><td>NEW</td><td>05/17/2017</td></tr>
<tr><td colspan="7">There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.0 before 1.1.0c that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected.</td></tr>
<tr><td>CVE-2017-3733</td><td>MEDIUM</td><td>5.0</td><td>2.9</td><td>10.0</td><td>NEW</td><td>05/17/2017</td></tr>
<tr><td colspan="7">During a renegotiation handshake if the Encrypt-Then-Mac extension is negotiated where it was not in the original handshake (or vice-versa) then this can cause OpenSSL 1.1.0 before 1.1.0e to crash (dependent on ciphersuite). Both clients and servers are affected.</td></tr>
</table>

Generated for **HPE Security**
Fortify on Demand

NOTE*: This report lists* ***only*** *the vulnerable components for this Hub project. To view a complete list of Open Source components identified, go to C Demo Project 3.4.*