Vulnerabilidades e Exposições Comuns - Rev 01 - 2021-10-29

Qt

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2013-0254	264			06/02/2013	16/06/2021	3,6	None	Local	Low	Not required	Partial	Partial	None	The QSharedMemory class in Qt 5.0.0, 4.8.x before 4.8.5, 4.7.x before 4.7.6, and other versions including 4.4.0 uses weak permissions (world-readable and world-writable) for shared memory segments, which allows local users to read sensitive information or modify critical program data, as demonstrated by reading a pixmap being sent to an X server.
2	CVE-2012-6093	310			24/02/2013	16/06/2021	4,3	None	Remote	Medium	Not required	Partial	None	None	The QSslSocket::sslErrors function in Qt before 4.6.5, 4.7.x before 4.7.6, 4.8.x before 4.8.5, when using certain versions of openSSL, uses an "incompatible structure layout" that can read memory from the wrong location, which causes Qt to report an incorrect error when certificate validation fails and might cause users to make unsafe security decisions to accept a certificate.
3	CVE-2012-5624	200			24/02/2013	16/06/2021	4,3	None	Remote	Medium	Not required	Partial	None	None	The XMLHttpRequest object in Qt before 4.8.4 enables http redirection to the file scheme, which allows man-in-the-middle attackers to force the read of arbitrary local files and possibly obtain sensitive information via a file: URL to a QML application.
4	CVE-2009-2700	20			02/09/2009	16/06/2021	4,3	None	Remote	Medium	Not required	None	Partial	None	src/network/ssl/qsslcertificate.cpp in Nokia Trolltech Qt 4.x does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

zlib

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2016-9843	189			23/05/2017	28/07/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.
2	CVE-2016-9842	189			23/05/2017	28/07/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers.
3	CVE-2016-9841	189			23/05/2017	28/07/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.
4	CVE-2016-9840	189			23/05/2017	28/07/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.
5	CVE-2005-2096			DoS Overflow	06/07/2005	19/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	zlib 1.2 and later versions allows remote attackers to cause a denial of service (crash) via a crafted compressed stream with an incomplete code description of a length greater than 1, which leads to a buffer overflow, as demonstrated using a crafted PNG file.
6	CVE-2005-1849			DoS	26/07/2005	19/10/2018	5	None	Remote	Low	Not required	None	None	Partial	inftrees.h in zlib 1.2.2 allows remote attackers to cause a denial of service (application crash) via an invalid file that causes a large dynamic tree to be produced.
7	CVE-2004-0797			DoS	20/10/2004	11/07/2017	2,1	None	Local	Low	Not required	None	None	Partial	The error handling in the (1) inflate and (2) inflateBack functions in ZLib compression library 1.2.x allows local users to cause a denial of service (application crash).
8	CVE-2003-0107			DoS Exec Code Overflow	07/03/2003	03/01/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflow in the gzprintf function in zlib 1.1.4, when zlib is compiled without vsnprintf or when long inputs are truncated using vsnprintf, allows attackers to cause a denial of service or possibly execute arbitrary code.
9	CVE-2002-0059			Exec Code	15/03/2002	03/05/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The decompression algorithm in zlib 1.1.3 and earlier, as used in many different utilities and packages, causes inflateEnd to release certain memory more than once (a "double free"), which may allow local and remote attackers to execute arbitrary code via a block of malformed compression data.

openssl

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2021-38604	476			12/08/2021	07/10/2021	5	None	Remote	Low	Not required	None	None	Partial	In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.
2	CVE-2021-35942	190		DoS	22/07/2021	21/09/2021	6,4	None	Remote	Low	Not required	Partial	None	Partial	The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.
3	CVE-2021-33574	416		DoS	25/05/2021	07/07/2021	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.
4	CVE-2021-27645	415		DoS	24/02/2021	06/07/2021	1,9	None	Local	Medium	Not required	None	None	Partial	The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.
5	CVE-2021-3326	617		DoS	27/01/2021	06/07/2021	5	None	Remote	Low	Not required	None	None	Partial	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
6	CVE-2020-29573	787		Overflow	06/12/2020	26/01/2021	5	None	Remote	Low	Not required	None	None	Partial	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-i
7	CVE-2020-29562	617		DoS	04/12/2020	19/03/2021	2,1	None	Remote	High	???	None	None	Partial	The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
8	CVE-2020-27618	835		DoS	26/02/2021	06/07/2021	2,1	None	Local	Low	Not required	None	None	Partial	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.
9	CVE-2020-10029	119		Overflow	04/03/2020	21/07/2021	2,1	None	Local	Low	Not required	None	None	Partial	The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.
10	CVE-2020-6096	191		Exec Code	01/04/2020	04/03/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, t
11	CVE-2020-1752	416		Exec Code	30/04/2020	29/06/2021	3,7	None	Local	High	Not required	Partial	Partial	Partial	A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.
12	CVE-2020-1751	787		DoS Exec Code	17/04/2020	09/07/2020	5,9	None	Local	Medium	Not required	Partial	Partial	Complete	An out-of-bounds write vulnerability was found in glibc before 2.31 when handling signal trampolines on PowerPC. Specifically, the backtrace function did not properly check the array bounds when storing the frame address, resulting in a denial of service or potential code execution. The highest threat from this vulnerability is to system availability.
13	CVE-2019-101002	330		Bypass	15/07/2019	16/11/2020	5	None	Remote	Low	Not required	Partial	None	None	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability."
14	CVE-2019-101002	200		Bypass +Info	15/07/2019	16/11/2020	5	None	Remote	Low	Not required	Partial	None	None	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
15	CVE-2019-1010023			Exec Code	15/07/2019	16/11/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	** DISPUTED ** GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
16	CVE-2019-101002	119		Overflow Bypass	15/07/2019	10/06/2021	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
17	CVE-2019-25013	125			04/01/2021	06/07/2021	7,1	None	Remote	Medium	Not required	None	None	Complete	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
18	CVE-2019-19126	200		Bypass +Info	19/11/2019	21/07/2021	2,1	None	Local	Low	Not required	Partial	None	None	On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.
19	CVE-2019-9192	674			26/02/2019	24/08/2020	5	None	Remote	Low	Not required	None	None	Partial	** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.
20	CVE-2019-9169	125			26/02/2019	09/07/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.
21	CVE-2019-7309				03/02/2019	24/08/2020	2,1	None	Local	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return zero (indicating that the inputs are equal) because the RDX most significant bit is mishandled.
22	CVE-2019-6488	404			18/01/2019	13/06/2020	4,6	None	Local	Low	Not required	Partial	Partial	Partial	The string component in the GNU C Library (aka glibc or libc6) through 2.28, when running on the x32 architecture, incorrectly attempts to use a 64-bit register for size_t in assembly codes, which can lead to a segmentation fault or possibly unspecified other impact, as demonstrated by a crash in __memmove_avx_unaligned_erms in sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S during a memcpy.
23	CVE-2018-100000	787		Exec Code	31/01/2018	03/10/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
24	CVE-2018-20796	674			26/02/2019	05/11/2019	5	None	Remote	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.
25	CVE-2018-19591	20			04/12/2018	09/07/2020	5	None	Remote	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) through 2.28, attempting to resolve a crafted hostname via getaddrinfo() leads to the allocation of a socket descriptor that is not closed. This is related to the if_nametoindex() function.
26	CVE-2018-11237	787		Overflow	18/05/2018	24/08/2020	4,6	None	Local	Low	Not required	Partial	Partial	Partial	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
27	CVE-2018-11236	787		Exec Code Overflow	18/05/2018	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.
28	CVE-2018-6551	787			02/02/2018	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.
29	CVE-2018-6485	787		Overflow	01/02/2018	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
30	CVE-2017-100040	119		Overflow	01/02/2018	04/04/2019	6,9	None	Local	Medium	Not required	Complete	Complete	Complete	A buffer overflow in glibc 2.5 (released on September 29, 2006) and can be triggered through the LD_LIBRARY_PATH environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
31	CVE-2017-100040	772			01/02/2018	03/10/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	A memory leak in glibc 2.1.1 (released on May 24, 1999) can be reached and amplified through the LD_HWCAP_MASK environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
32	CVE-2017-100036	119		Exec Code Overflow	19/06/2017	15/10/2020	7,2	None	Local	Low	Not required	Complete	Complete	Complete	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
33	CVE-2017-17426	190		Overflow	05/12/2017	15/12/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check.
34	CVE-2017-16997	426			18/12/2017	15/10/2020	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileg
35	CVE-2017-15804	119		Overflow	22/10/2017	20/06/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
36	CVE-2017-15671	772		DoS	20/10/2017	03/10/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TILDE, could skip freeing allocated memory when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak).
37	CVE-2017-15670	119		Overflow	20/10/2017	20/06/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
38	CVE-2017-12133	416			07/09/2017	09/07/2020	4,3	None	Remote	Medium	Not required	None	Partial	None	Use-after-free vulnerability in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) before 2.26 allows remote attackers to have unspecified impact via vectors related to error path.
39	CVE-2017-12132	770			01/08/2017	03/10/2019	4,3	None	Remote	Medium	Not required	None	Partial	None	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
40	CVE-2017-8804	502		DoS	07/05/2017	26/08/2020	7,8	None	Remote	Low	Not required	None	None	Complete	** DISPUTED ** The xdr_bytes and xdr_string functions in the GNU C Library (aka glibc or libc6) 2.25 mishandle failures of buffer deserialization, which allows remote attackers to cause a denial of service (virtual memory allocation, or memory consumption if an overcommit setting is not used) via a crafted UDP packet to port 111, a related issue to CVE-2017-8779. NOTE: [Information provided from upstream and references]
41	CVE-2016-10739	20			21/01/2019	06/08/2019	4,6	None	Local	Low	Not required	Partial	Partial	Partial	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
42	CVE-2016-10228	20		DoS	02/03/2017	25/02/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.
43	CVE-2016-6323	284		DoS	07/10/2016	30/10/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
44	CVE-2016-5417	399		DoS	17/02/2017	17/02/2017	5	None	Remote	Low	Not required	None	None	Partial	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.
45	CVE-2016-4429	787		DoS Overflow	10/06/2016	20/07/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
46	CVE-2016-3706	20		DoS Overflow	10/06/2016	29/10/2020	5	None	Remote	Low	Not required	None	None	Partial	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.
47	CVE-2016-3075	119		DoS Overflow	01/06/2016	30/10/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
48	CVE-2016-1234	119		DoS Overflow	01/06/2016	01/09/2021	5	None	Remote	Low	Not required	None	None	Partial	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.
49	CVE-2015-8985	19		DoS	20/03/2017	31/03/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (assertion failure and application crash) via vectors related to extended regular expression processing.
50	CVE-2015-8984	125		DoS	20/03/2017	22/03/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.
51	CVE-2016-2180	125		DoS	01/08/2016	27/12/2019	5	None	Remote	Low	Not required	None	None	Partial	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.
52	CVE-2016-2179	399		DoS	16/09/2016	27/12/2019	5	None	Remote	Low	Not required	None	None	Partial	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.
53	CVE-2016-2178	200			20/06/2016	27/12/2019	2,1	None	Local	Low	Not required	Partial	None	None	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.
54	CVE-2016-2177	190		DoS Overflow	20/06/2016	27/12/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
55	CVE-2016-2176	119		DoS Overflow +Info	05/05/2016	19/07/2018	6,4	None	Remote	Low	Not required	Partial	None	Partial	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.
56	CVE-2016-2109	399		DoS	05/05/2016	19/07/2018	7,8	None	Remote	Low	Not required	None	None	Complete	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.
57	CVE-2016-2108	119		DoS Exec Code Overflow Mem. Corr.	05/05/2016	05/01/2018	10	None	Remote	Low	Not required	Complete	Complete	Complete	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.
58	CVE-2016-2107	310			05/05/2016	30/10/2018	2,6	None	Remote	High	Not required	Partial	None	None	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.
59	CVE-2016-2106	189		DoS Overflow Mem. Corr.	05/05/2016	19/07/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
60	CVE-2016-2105	189		DoS Overflow Mem. Corr.	05/05/2016	21/02/2019	5	None	Remote	Low	Not required	None	None	Partial	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.
61	CVE-2016-0800	310			01/03/2016	30/11/2018	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
62	CVE-2016-0799	119		DoS Overflow	03/03/2016	05/01/2018	10	None	Remote	Low	Not required	Complete	Complete	Complete	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.
63	CVE-2016-0798	399		DoS	03/03/2016	21/11/2017	7,8	None	Remote	Low	Not required	None	None	Complete	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.
64	CVE-2016-0797			DoS Overflow Mem. Corr.	03/03/2016	05/01/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
65	CVE-2016-0705			DoS Mem. Corr.	03/03/2016	20/02/2019	10	None	Remote	Low	Not required	Complete	Complete	Complete	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.
66	CVE-2016-0704	200			02/03/2016	18/01/2018	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
67	CVE-2016-0703	200			02/03/2016	18/01/2018	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
68	CVE-2016-0702	200			03/03/2016	05/01/2018	1,9	None	Local	Medium	Not required	Partial	None	None	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.
69	CVE-2016-0701	200			15/02/2016	20/10/2020	2,6	None	Remote	High	Not required	Partial	None	None	The DH_check_pub_key function in crypto/dh/dh_check.c in OpenSSL 1.0.2 before 1.0.2f does not ensure that prime numbers are appropriate for Diffie-Hellman (DH) key exchange, which makes it easier for remote attackers to discover a private DH exponent by making multiple handshakes with a peer that chose an inappropriate number, as demonstrated by a number in an X9.42 file.
70	CVE-2015-4000	310			21/05/2015	23/07/2021	4,3	None	Remote	Medium	Not required	None	Partial	None	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.
71	CVE-2015-3216	189		DoS	07/07/2015	05/01/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	Race condition in a certain Red Hat patch to the PRNG lock implementation in the ssleay_rand_bytes function in OpenSSL, as distributed in openssl-1.0.1e-25.el7 in Red Hat Enterprise Linux (RHEL) 7 and other products, allows remote attackers to cause a denial of service (application crash) by establishing many TLS sessions to a multithreaded server, leading to use of a negative value for a certain length field.
72	CVE-2015-3197	310			15/02/2016	21/11/2017	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
73	CVE-2015-3196	362		DoS	06/12/2015	13/06/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
74	CVE-2015-3195	200			06/12/2015	19/01/2021	5	None	Remote	Low	Not required	None	None	Partial	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.
75	CVE-2015-3194			DoS	06/12/2015	07/02/2019	5	None	Remote	Low	Not required	None	None	Partial	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.
76	CVE-2015-3193	200			06/12/2015	30/11/2017	5	None	Remote	Low	Not required	Partial	None	None	The Montgomery squaring implementation in crypto/bn/asm/x86_64-mont5.pl in OpenSSL 1.0.2 before 1.0.2e on the x86_64 platform, as used by the BN_mod_exp function, mishandles carry propagation and produces incorrect output, which makes it easier for remote attackers to obtain sensitive private-key information via an attack against use of a (1) Diffie-Hellman (DH) or (2) Diffie-Hellman Ephemeral (DHE) ciphersuite.
77	CVE-2015-1794	189		DoS	06/12/2015	14/09/2017	5	None	Remote	Low	Not required	None	None	Partial	The ssl3_get_key_exchange function in ssl/s3_clnt.c in OpenSSL 1.0.2 before 1.0.2e allows remote servers to cause a denial of service (segmentation fault) via a zero p value in an anonymous Diffie-Hellman (DH) ServerKeyExchange message.
78	CVE-2015-1793	254			09/07/2015	30/11/2018	6,4	None	Remote	Low	Not required	Partial	Partial	None	The X509_verify_cert function in crypto/x509/x509_vfy.c in OpenSSL 1.0.1n, 1.0.1o, 1.0.2b, and 1.0.2c does not properly process X.509 Basic Constraints cA values during identification of alternative certificate chains, which allows remote attackers to spoof a Certification Authority role and trigger unintended certificate verifications via a valid leaf certificate.
79	CVE-2015-1792	399		DoS	12/06/2015	15/11/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
80	CVE-2015-1791	362		DoS	12/06/2015	15/11/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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.
81	CVE-2015-1790			DoS	12/06/2015	20/10/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
82	CVE-2015-1789	119		DoS Overflow	12/06/2015	15/11/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
83	CVE-2015-1788	399		DoS	12/06/2015	15/11/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
84	CVE-2015-1787	20		DoS	19/03/2015	29/11/2018	2,6	None	Remote	High	Not required	None	None	Partial	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.
85	CVE-2015-0293	20		DoS	19/03/2015	18/01/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
86	CVE-2015-0292	119		DoS Overflow Mem. Corr.	19/03/2015	15/11/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
87	CVE-2015-0291			DoS	19/03/2015	29/11/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
88	CVE-2015-0290	17		DoS	19/03/2015	29/11/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
89	CVE-2015-0289			DoS	19/03/2015	20/10/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
90	CVE-2015-0288			DoS	19/03/2015	15/11/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
91	CVE-2015-0287	17		DoS Mem. Corr.	19/03/2015	15/11/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
92	CVE-2015-0286	17		DoS	19/03/2015	05/01/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
93	CVE-2015-0285	310			19/03/2015	29/11/2018	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
94	CVE-2015-0209			DoS Mem. Corr.	19/03/2015	05/01/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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.
95	CVE-2015-0208			DoS	19/03/2015	29/11/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
96	CVE-2015-0207			DoS	19/03/2015	29/11/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
97	CVE-2015-0206	119		DoS Overflow	09/01/2015	20/10/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
98	CVE-2015-0205	310			09/01/2015	15/11/2017	5	None	Remote	Low	Not required	None	Partial	None	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.
99	CVE-2015-0204	310			09/01/2015	19/07/2018	4,3	None	Remote	Medium	Not required	None	Partial	None	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.
100	CVE-2014-8275	310			09/01/2015	15/11/2017	5	None	Remote	Low	Not required	None	Partial	None	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.
101	CVE-2014-8176	119		DoS Overflow Mem. Corr.	12/06/2015	05/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
102	CVE-2014-5139			DoS	13/08/2014	07/01/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
103	CVE-2014-3572	310			09/01/2015	15/11/2017	5	None	Remote	Low	Not required	None	Partial	None	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.
104	CVE-2014-3571			DoS	09/01/2015	20/10/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
105	CVE-2014-3570	310			09/01/2015	15/11/2017	5	None	Remote	Low	Not required	Partial	None	None	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.
106	CVE-2014-3569			DoS	24/12/2014	15/11/2017	5	None	Remote	Low	Not required	None	None	Partial	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.
107	CVE-2014-3568	310		Bypass	19/10/2014	15/11/2017	4,3	None	Remote	Medium	Not required	None	Partial	None	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.
108	CVE-2014-3567	20		DoS	19/10/2014	15/11/2017	7,1	None	Remote	Medium	Not required	None	None	Complete	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.
109	CVE-2014-3566	310			15/10/2014	31/08/2021	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
110	CVE-2014-3513	20		DoS	19/10/2014	03/01/2017	7,1	None	Remote	Medium	Not required	None	None	Complete	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.
111	CVE-2014-3512	119		DoS Overflow	13/08/2014	29/08/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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 parameter.
112	CVE-2014-3511				13/08/2014	15/11/2017	4,3	None	Remote	Medium	Not required	None	Partial	None	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.

113	CVE-2014-3510			DoS	13/08/2014	29/08/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
114	CVE-2014-3509	362		DoS	13/08/2014	15/11/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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.
115	CVE-2014-3508	200			13/08/2014	15/11/2017	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
116	CVE-2014-3507	399		DoS	13/08/2014	29/08/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
117	CVE-2014-3506	399		DoS	13/08/2014	29/08/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
118	CVE-2014-3505			DoS	13/08/2014	07/01/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
119	CVE-2014-3470	310		DoS	05/06/2014	22/04/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
120	CVE-2014-0224	326			05/06/2014	28/07/2020	5,8	None	Remote	Medium	Not required	Partial	Partial	None	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.
121	CVE-2014-0221	399		DoS	05/06/2014	22/04/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
122	CVE-2014-0198			DoS	06/05/2014	09/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
123	CVE-2014-0195	119		DoS Exec Code Overflow	05/06/2014	22/04/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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.
124	CVE-2014-0160	119	2	Overflow +Info	07/04/2014	28/07/2020	5	None	Remote	Low	Not required	Partial	None	None	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.
125	CVE-2014-0076	310			25/03/2014	16/12/2017	1,9	None	Local	Medium	Not required	Partial	None	None	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.
126	CVE-2013-6450	310		DoS	01/01/2014	09/10/2018	5,8	None	Remote	Medium	Not required	None	Partial	Partial	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.
127	CVE-2013-6449	310		DoS	23/12/2013	09/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
128	CVE-2013-4353	20		DoS	09/01/2014	07/01/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
129	CVE-2013-0169	310			08/02/2013	09/10/2019	2,6	None	Remote	High	Not required	Partial	None	None	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.
130	CVE-2013-0166	310		DoS	08/02/2013	09/08/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
131	CVE-2012-2686	310		DoS	08/02/2013	09/08/2018	5	None	Remote	Low	Not required	None	None	Partial	crypto/evp/e_aes_cbc_hmac_sha1.c in the AES-NI functionality in the TLS 1.1 and 1.2 implementations in OpenSSL 1.0.1 before 1.0.1d allows remote attackers to cause a denial of service (application crash) via crafted CBC data.
132	CVE-2012-2333	189		DoS	14/05/2012	05/01/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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.
133	CVE-2012-2131	189		DoS Overflow Mem. Corr.	24/04/2012	05/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Multiple integer signedness errors in crypto/buffer/buffer.c in OpenSSL 0.9.8v allow 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. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-2110.
134	CVE-2012-2110	119	1	DoS Overflow Mem. Corr.	19/04/2012	05/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
135	CVE-2012-1165	399		DoS	15/03/2012	13/01/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
136	CVE-2012-0884	310			13/03/2012	10/01/2018	5	None	Remote	Low	Not required	Partial	None	None	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.
137	CVE-2012-0050	399		DoS	19/01/2012	23/08/2016	5	None	Remote	Low	Not required	None	None	Partial	OpenSSL 0.9.8s and 1.0.0f does not properly support DTLS applications, which allows remote attackers to cause a denial of service (crash) via unspecified vectors related to an out-of-bounds read. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-4108.
138	CVE-2012-0027	399		DoS	06/01/2012	26/03/2014	5	None	Remote	Low	Not required	None	None	Partial	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.
139	CVE-2011-5095	310			20/06/2012	21/06/2012	4	None	Remote	High	Not required	Partial	Partial	None	The Diffie-Hellman key-exchange implementation in OpenSSL 0.9.8, when FIPS mode is enabled, does not properly validate a public parameter, which makes it easier for man-in-the-middle attackers to obtain the shared secret key by modifying network traffic, a related issue to CVE-2011-1923.
140	CVE-2011-4619	399		DoS	06/01/2012	23/08/2016	5	None	Remote	Low	Not required	None	None	Partial	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.
141	CVE-2011-4577	399		DoS	06/01/2012	26/03/2014	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
142	CVE-2011-4576	310			06/01/2012	23/08/2016	5	None	Remote	Low	Not required	Partial	None	None	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.
143	CVE-2011-4354	310			27/01/2012	06/11/2012	5,8	None	Remote	Medium	Not required	Partial	Partial	None	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.
144	CVE-2011-4109	399			06/01/2012	29/08/2017	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	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.
145	CVE-2011-4108	310			06/01/2012	23/08/2016	4,3	None	Remote	Medium	Not required	Partial	None	None	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.
146	CVE-2011-3210	399		DoS	22/09/2011	26/03/2014	5	None	Remote	Low	Not required	None	None	Partial	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.
147	CVE-2011-3207	264		Bypass	22/09/2011	26/03/2014	5	None	Remote	Low	Not required	None	Partial	None	crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier for remote attackers to bypass CRL validation by using a nextUpdate value corresponding to a time in the past.
148	CVE-2011-1945	310			31/05/2011	06/06/2013	2,6	None	Remote	High	Not required	Partial	None	None	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.
149	CVE-2011-1473	264		DoS	16/06/2012	20/04/2021	5	None	Remote	Low	Not required	None	None	Partial	** 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. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation whe
150	CVE-2011-0014	399		DoS +Info	19/02/2011	19/09/2017	5	None	Remote	Low	Not required	None	None	Partial	ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, via a malformed ClientHello handshake message that triggers an out-of-bounds memory access, aka "OCSP stapling vulnerability."
151	CVE-2010-5298	362		DoS	14/04/2014	10/10/2018	4	None	Remote	High	Not required	None	Partial	Partial	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.
152	CVE-2010-4252	287		Bypass	06/12/2010	19/09/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
153	CVE-2010-4180				06/12/2010	19/09/2017	4,3	None	Remote	Medium	Not required	None	Partial	None	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.
154	CVE-2010-3864	362		Exec Code Overflow	17/11/2010	10/10/2018	7,6	None	Remote	High	Not required	Complete	Complete	Complete	Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.
155	CVE-2010-2939	399		DoS Exec Code	17/08/2010	10/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	Double free vulnerability in the ssl3_get_key_exchange function in the OpenSSL client (ssl/s3_clnt.c) in OpenSSL 1.0.0a, 0.9.8, 0.9.7, and possibly other versions, when using ECDH, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted private key with an invalid prime. NOTE: some sources refer to this as a use-after-free issue.
156	CVE-2010-1633	264		Bypass +Info	03/06/2010	26/03/2014	6,4	None	Remote	Low	Not required	Partial	Partial	None	RSA verification recovery in the EVP_PKEY_verify_recover function in OpenSSL 1.x before 1.0.0a, as used by pkeyutl and possibly other applications, returns uninitialized memory upon failure, which might allow context-dependent attackers to bypass intended key requirements or obtain sensitive information via unspecified vectors. NOTE: some of these details are obtained from third party information.
157	CVE-2010-0742	310		Exec Code	03/06/2010	19/09/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
158	CVE-2010-0740	20		DoS	26/03/2010	10/10/2018	5	None	Remote	Low	Not required	None	None	Partial	The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information.
159	CVE-2010-0433	20		DoS	05/03/2010	10/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
160	CVE-2009-4355	399		DoS	14/01/2010	19/09/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
161	CVE-2009-3555	310			09/11/2009	05/02/2021	5,8	None	Remote	Medium	Not required	None	Partial	Partial	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 sessio
162	CVE-2009-3245	20			05/03/2010	19/09/2017	10	None	Remote	Low	Not required	Complete	Complete	Complete	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.
163	CVE-2009-2409	310			30/07/2009	10/10/2018	5,1	None	Remote	High	Not required	Partial	Partial	Partial	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.
164	CVE-2009-1387	399		DoS	04/06/2009	29/09/2017	5	None	Remote	Low	Not required	None	None	Partial	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."
165	CVE-2009-1386			DoS	04/06/2009	29/09/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
166	CVE-2009-1379	399		DoS	19/05/2009	29/09/2017	5	None	Remote	Low	Not required	None	None	Partial	Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allows remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact via a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate.
167	CVE-2009-1378	399		DoS	19/05/2009	29/09/2017	5	None	Remote	Low	Not required	None	None	Partial	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."
168	CVE-2009-1377	119		DoS Overflow	19/05/2009	29/09/2017	5	None	Remote	Low	Not required	None	None	Partial	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."
169	CVE-2009-0789	189		DoS	27/03/2009	17/08/2017	5	None	Remote	Low	Not required	None	None	Partial	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.
170	CVE-2009-0653	287			20/02/2009	25/06/2009	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	OpenSSL, probably 0.9.6, does not verify the Basic Constraints for an intermediate CA-signed certificate, which allows remote attackers to spoof the certificates of trusted sites via a man-in-the-middle attack, a related issue to CVE-2002-0970.
171	CVE-2009-0591	287			27/03/2009	17/08/2017	2,6	None	Remote	High	Not required	None	Partial	None	The CMS_verify function in OpenSSL 0.9.8h through 0.9.8j, when CMS is enabled, does not properly handle errors associated with malformed signed attributes, which allows remote attackers to repudiate a signature that originally appeared to be valid but was actually invalid.
172	CVE-2009-0590	119		DoS Overflow	27/03/2009	03/11/2020	5	None	Remote	Low	Not required	None	None	Partial	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.
173	CVE-2008-7270	310			06/12/2010	06/04/2012	4,3	None	Remote	Medium	Not required	None	Partial	None	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.
174	CVE-2008-5077	20		Bypass	07/01/2009	11/10/2018	5,8	None	Remote	Medium	Not required	None	Partial	Partial	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.
175	CVE-2008-1678	399		DoS	10/07/2008	29/09/2017	5	None	Remote	Low	Not required	None	None	Partial	Memory leak in the zlib_stateful_init function in crypto/comp/c_zlib.c in libssl in OpenSSL 0.9.8f through 0.9.8h allows remote attackers to cause a denial of service (memory consumption) via multiple calls, as demonstrated by initial SSL client handshakes to the Apache HTTP Server mod_ssl that specify a compression algorithm.
176	CVE-2008-0891	189		DoS	29/05/2008	08/08/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	Double free vulnerability in OpenSSL 0.9.8f and 0.9.8g, when the TLS server name extensions are enabled, allows remote attackers to cause a denial of service (crash) via a malformed Client Hello packet. NOTE: some of these details are obtained from third party information.
177	CVE-2007-5502	310		Bypass	01/12/2007	29/07/2017	6,4	None	Remote	Low	Not required	Partial	Partial	None	The PRNG implementation for the OpenSSL FIPS Object Module 1.1.1 does not perform auto-seeding during the FIPS self-test, which generates random data that is more predictable than expected and makes it easier for attackers to bypass protection mechanisms that rely on the randomness.
178	CVE-2007-5135	189		Exec Code	27/09/2007	15/10/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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. As of 20071012, it is unknown whether code execution is possible.
179	CVE-2007-4995	189		Exec Code	13/10/2007	15/10/2018	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	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.
180	CVE-2007-3108				08/08/2007	16/10/2018	1,2	None	Local	High	Not required	Partial	None	None	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.
181	CVE-2006-7250			DoS	29/02/2012	06/01/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
182	CVE-2006-4343	476		DoS	28/09/2006	17/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	The get_server_hello function in the SSLv2 client code in OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows remote servers to cause a denial of service (client crash) via unknown vectors that trigger a null pointer dereference.
183	CVE-2006-4339	310			05/09/2006	17/10/2018	4,3	None	Remote	Medium	Not required	Partial	None	None	OpenSSL before 0.9.7, 0.9.7 before 0.9.7k, and 0.9.8 before 0.9.8c, when using an RSA key with exponent 3, removes PKCS-1 padding before generating a hash, which allows remote attackers to forge a PKCS #1 v1.5 signature that is signed by that RSA key and prevents OpenSSL from correctly verifying X.509 and other certificates that use PKCS #1.
184	CVE-2006-3738	119		Overflow	28/09/2006	17/10/2018	10	None	Remote	Low	Not required	Complete	Complete	Complete	Buffer overflow in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions has unspecified impact and remote attack vectors involving a long list of ciphers.
185	CVE-2006-2940	399		DoS	28/09/2006	18/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier versions allows attackers to cause a denial of service (CPU consumption) via parasitic public keys with large (1) "public exponent" or (2) "public modulus" values in X.509 certificates that require extra time to process when using RSA signature verification.
186	CVE-2006-2937	399		DoS	28/09/2006	18/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	OpenSSL 0.9.7 before 0.9.7l and 0.9.8 before 0.9.8d allows remote attackers to cause a denial of service (infinite loop and memory consumption) via malformed ASN.1 structures that trigger an improperly handled error condition.
187	CVE-2005-2969				18/10/2005	03/05/2018	5	None	Remote	Low	Not required	None	Partial	None	The SSL/TLS server implementation in OpenSSL 0.9.7 before 0.9.7h and 0.9.8 before 0.9.8a, when using the SSL_OP_MSIE_SSLV2_RSA_PADDING option, disables a verification step that is required for preventing protocol version rollback attacks, which allows remote attackers to force a client and server to use a weaker protocol than needed via a man-in-the-middle attack.
188	CVE-2005-2946	310			16/09/2005	07/01/2009	5	None	Remote	Low	Not required	None	Partial	None	The default configuration on OpenSSL before 0.9.8 uses MD5 for creating message digests instead of a more cryptographically strong algorithm, which makes it easier for remote attackers to forge certificates with a valid certificate authority signature.
189	CVE-2005-1797				26/05/2005	05/09/2008	5,1	None	Remote	High	Not required	Partial	Partial	Partial	The design of Advanced Encryption Standard (AES), aka Rijndael, allows remote attackers to recover AES keys via timing attacks on S-box lookups, which are difficult to perform in constant time in AES implementations.
190	CVE-2004-0975				09/02/2005	11/10/2017	2,1	None	Local	Low	Not required	None	Partial	None	The der_chop script in the openssl package in Trustix Secure Linux 1.5 through 2.1 and other operating systems allows local users to overwrite files via a symlink attack on temporary files.
191	CVE-2003-0545	119		DoS Exec Code Overflow	17/11/2003	03/05/2018	10	None	Remote	Low	Not required	Complete	Complete	Complete	Double free vulnerability in OpenSSL 0.9.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an SSL client certificate with a certain invalid ASN.1 encoding.
192	CVE-2003-0544			DoS	17/11/2003	03/05/2018	5	None	Remote	Low	Not required	None	None	Partial	OpenSSL 0.9.6 and 0.9.7 does not properly track the number of characters in certain ASN.1 inputs, which allows remote attackers to cause a denial of service (crash) via an SSL client certificate that causes OpenSSL to read past the end of a buffer when the long form is used.
193	CVE-2003-0543			DoS Overflow	17/11/2003	03/05/2018	5	None	Remote	Low	Not required	None	None	Partial	Integer overflow in OpenSSL 0.9.6 and 0.9.7 allows remote attackers to cause a denial of service (crash) via an SSL client certificate with certain ASN.1 tag values.
194	CVE-2003-0147				31/03/2003	19/10/2018	5	None	Remote	Low	Not required	Partial	None	None	OpenSSL does not use RSA blinding by default, which allows local and remote attackers to obtain the server's private key by determining factors using timing differences on (1) the number of extra reductions during Montgomery reduction, and (2) the use of different integer multiplication algorithms ("Karatsuba" and normal).
195	CVE-2003-0131				24/03/2003	19/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The SSL and TLS components for OpenSSL 0.9.6i and earlier, 0.9.7, and 0.9.7a allow remote attackers to perform an unauthorized RSA private key operation via a modified Bleichenbacher attack that uses a large number of SSL or TLS connections using PKCS #1 v1.5 padding that cause OpenSSL to leak information regarding the relationship between ciphertext and the associated plaintext, aka the "Klima-Pokorny-Rosa attack."
196	CVE-2003-0078				03/03/2003	18/10/2016	5	None	Remote	Low	Not required	Partial	None	None	ssl3_get_record in s3_pkt.c for OpenSSL before 0.9.7a and 0.9.6 before 0.9.6i does not perform a MAC computation if an incorrect block cipher padding is used, which causes an information leak (timing discrepancy) that may make it easier to launch cryptographic attacks that rely on distinguishing between padding and MAC verification errors, possibly leading to extraction of the original plaintext, aka the "Vaudenay timing attack."
197	CVE-2002-1568			DoS Overflow	17/11/2003	18/10/2016	5	None	Remote	Low	Not required	None	None	Partial	OpenSSL 0.9.6e uses assertions when detecting buffer overflow attacks instead of less severe mechanisms, which allows remote attackers to cause a denial of service (crash) via certain messages that cause OpenSSL to abort from a failed assertion, as demonstrated using SSLv2 CLIENT_MASTER_KEY messages, which are not properly handled in s2_srvr.c.
198	CVE-2002-0659			DoS	12/08/2002	10/09/2008	5	None	Remote	Low	Not required	None	None	Partial	The ASN1 library in OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, allows remote attackers to cause a denial of service via invalid encodings.
199	CVE-2002-0657			Exec Code Overflow	12/08/2002	10/09/2008	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflow in OpenSSL 0.9.7 before 0.9.7-beta3, with Kerberos enabled, allows attackers to execute arbitrary code via a long master key.
200	CVE-2002-0656			Exec Code Overflow	12/08/2002	10/09/2008	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflows in OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, allow remote attackers to execute arbitrary code via (1) a large client master key in SSL2 or (2) a large session ID in SSL3.
201	CVE-2002-0655			DoS Exec Code	12/08/2002	10/09/2008	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, does not properly handle ASCII representations of integers on 64 bit platforms, which could allow attackers to cause a denial of service and possibly execute arbitrary code.
202	CVE-2001-1141				10/07/2001	10/10/2017	5	None	Remote	Low	Not required	Partial	None	None	The Pseudo-Random Number Generator (PRNG) in SSLeay and OpenSSL before 0.9.6b allows attackers to use the output of small PRNG requests to determine the internal state information, which could be used by attackers to predict future pseudo-random numbers.
203	CVE-2000-1254	310			05/05/2016	02/02/2017	5	None	Remote	Low	Not required	Partial	None	None	crypto/rsa/rsa_gen.c in OpenSSL before 0.9.6 mishandles C bitwise-shift operations that exceed the size of an expression, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging improper RSA key generation on 64-bit HP-UX platforms.
204	CVE-2000-0535				12/06/2000	10/09/2008	5	None	Remote	Low	Not required	None	Partial	None	OpenSSL 0.9.4 and OpenSSH for FreeBSD do not properly check for the existence of the /dev/random or /dev/urandom devices, which are absent on FreeBSD Alpha systems, which causes them to produce weak keys which may be more easily broken.
205	CVE-1999-0428	384		Bypass	22/03/1999	13/10/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	OpenSSL and SSLeay allow remote attackers to reuse SSL sessions and bypass access controls.

Linux Kernel

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2011-4330	119		DoS Exec Code Overflow	27/01/2012	16/04/2012	7,2	None	Local	Low	Not required	Complete	Complete	Complete	Stack-based buffer overflow in the hfs_mac2asc function in fs/hfs/trans.c in the Linux kernel 2.6 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via an HFS image with a crafted len field.
2	CVE-2011-4132	20		DoS	27/01/2012	29/12/2017	2,1	None	Local	Low	Not required	None	None	Partial	The cleanup_journal_tail function in the Journaling Block Device (JBD) functionality in the Linux kernel 2.6 allows local users to cause a denial of service (assertion error and kernel oops) via an ext3 or ext4 image with an "invalid log first block value."
3	CVE-2011-4110	264		DoS	27/01/2012	23/08/2016	2,1	None	Local	Low	Not required	None	None	Partial	The user_update function in security/keys/user_defined.c in the Linux kernel 2.6 allows local users to cause a denial of service (NULL pointer dereference and kernel oops) via vectors related to a user-defined key and "updating a negative key into a fully instantiated key."
4	CVE-2011-2203	264		DoS	27/01/2012	19/03/2012	2,1	None	Local	Low	Not required	None	None	Partial	The hfs_find_init function in the Linux kernel 2.6 allows local users to cause a denial of service (NULL pointer dereference and Oops) by mounting an HFS file system with a malformed MDB extent record.
5	CVE-2011-1162	200			27/01/2012	19/03/2012	2,1	None	Local	Low	Not required	Partial	None	None	The tpm_read function in the Linux kernel 2.6 does not properly clear memory, which might allow local users to read the results of the previous TPM command.
6	CVE-2010-3066			DoS	06/12/2010	10/10/2018	4,9	None	Local	Low	Not required	None	None	Complete	The io_submit_one function in fs/aio.c in the Linux kernel before 2.6.23 allows local users to cause a denial of service (NULL pointer dereference) via a crafted io_submit system call with an IOCB_FLAG_RESFD flag.
7	CVE-2010-0008	399		DoS	19/03/2010	10/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	The sctp_rcv_ootb function in the SCTP implementation in the Linux kernel before 2.6.23 allows remote attackers to cause a denial of service (infinite loop) via (1) an Out Of The Blue (OOTB) chunk or (2) a chunk of zero length.
8	CVE-2009-3726	399		DoS	09/11/2009	19/09/2017	7,8	None	Remote	Low	Not required	None	None	Complete	The nfs4_proc_lock function in fs/nfs/nfs4proc.c in the NFSv4 client in the Linux kernel before 2.6.31-rc4 allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) by sending a certain response containing incorrect file attributes, which trigger attempted use of an open file that lacks NFSv4 state.
9	CVE-2009-3624	310		DoS +Priv	02/11/2009	19/03/2012	4,6	None	Local	Low	Not required	Partial	Partial	Partial	The get_instantiation_keyring function in security/keys/keyctl.c in the KEYS subsystem in the Linux kernel before 2.6.32-rc5 does not properly maintain the reference count of a keyring, which allows local users to gain privileges or cause a denial of service (OOPS) via vectors involving calls to this function without specifying a keyring by ID, as demonstrated by a series of keyctl request2 and keyctl list commands.
10	CVE-2009-3613	399		DoS	19/10/2009	19/09/2017	7,8	None	Remote	Low	Not required	None	None	Complete	The swiotlb functionality in the r8169 driver in drivers/net/r8169.c in the Linux kernel before 2.6.27.22 allows remote attackers to cause a denial of service (IOMMU space exhaustion and system crash) by using jumbo frames for a large amount of network traffic, as demonstrated by a flood ping.
11	CVE-2009-2844	399		DoS	18/08/2009	19/03/2012	7,8	None	Remote	Low	Not required	None	None	Complete	cfg80211 in net/wireless/scan.c in the Linux kernel 2.6.30-rc1 and other versions before 2.6.31-rc6 allows remote attackers to cause a denial of service (crash) via a sequence of beacon frames in which one frame omits an SSID Information Element (IE) and the subsequent frame contains an SSID IE, which triggers a NULL pointer dereference in the cmp_ies function. NOTE: a potential weakness in the is_mesh function was also addressed, but the relevant condition did not exist in the code,
12	CVE-2009-2767	119		DoS Overflow +Priv	14/08/2009	17/08/2017	7,2	None	Local	Low	Not required	Complete	Complete	Complete	The init_posix_timers function in kernel/posix-timers.c in the Linux kernel before 2.6.31-rc6 allows local users to cause a denial of service (OOPS) or possibly gain privileges via a CLOCK_MONOTONIC_RAW clock_nanosleep call that triggers a NULL pointer dereference.
13	CVE-2009-2692	119	2	Overflow +Priv	14/08/2009	10/10/2018	7,2	None	Local	Low	Not required	Complete	Complete	Complete	The Linux kernel 2.6.0 through 2.6.30.4, and 2.4.4 through 2.4.37.4, does not initialize all function pointers for socket operations in proto_ops structures, which allows local users to trigger a NULL pointer dereference and gain privileges by using mmap to map page zero, placing arbitrary code on this page, and then invoking an unavailable operation, as demonstrated by the sendpage operation (sock_sendpage function) on a PF_PPPOX socket.
14	CVE-2009-2406	119		DoS Overflow +Priv	31/07/2009	30/10/2018	6,9	None	Local	Medium	Not required	Complete	Complete	Complete	Stack-based buffer overflow in the parse_tag_11_packet function in fs/ecryptfs/keystore.c in the eCryptfs subsystem in the Linux kernel before 2.6.30.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via vectors involving a crafted eCryptfs file, related to not ensuring that the key signature length in a Tag 11 packet is compatible with the key signature buffer size.
15	CVE-2009-1439	119		DoS Overflow	27/04/2009	10/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	Buffer overflow in fs/cifs/connect.c in CIFS in the Linux kernel 2.6.29 and earlier allows remote attackers to cause a denial of service (crash) via a long nativeFileSystem field in a Tree Connect response to an SMB mount request.
16	CVE-2009-1389	119		DoS Overflow Mem. Corr.	16/06/2009	30/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	Buffer overflow in the RTL8169 NIC driver (drivers/net/r8169.c) in the Linux kernel before 2.6.30 allows remote attackers to cause a denial of service (kernel memory corruption and crash) via a long packet.
17	CVE-2009-1385	189		DoS	04/06/2009	10/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	Integer underflow in the e1000_clean_rx_irq function in drivers/net/e1000/e1000_main.c in the e1000 driver in the Linux kernel before 2.6.30-rc8, the e1000e driver in the Linux kernel, and Intel Wired Ethernet (aka e1000) before 7.5.5 allows remote attackers to cause a denial of service (panic) via a crafted frame size.
18	CVE-2009-1360			DoS	22/04/2009	19/03/2012	7,1	None	Remote	Medium	Not required	None	None	Complete	The __inet6_check_established function in net/ipv6/inet6_hashtables.c in the Linux kernel before 2.6.29, when Network Namespace Support (aka NET_NS) is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via vectors involving IPv6 packets.
19	CVE-2009-1338	264		Bypass	22/04/2009	10/10/2018	4,6	None	Local	Low	Not required	Partial	Partial	Partial	The kill_something_info function in kernel/signal.c in the Linux kernel before 2.6.28 does not consider PID namespaces when processing signals directed to PID -1, which allows local users to bypass the intended namespace isolation, and send arbitrary signals to all processes in all namespaces, via a kill command.
20	CVE-2009-1337	264			22/04/2009	10/10/2018	4,4	None	Local	Medium	Not required	Partial	Partial	Partial	The exit_notify function in kernel/exit.c in the Linux kernel before 2.6.30-rc1 does not restrict exit signals when the CAP_KILL capability is held, which allows local users to send an arbitrary signal to a process by running a program that modifies the exit_signal field and then uses an exec system call to launch a setuid application.
21	CVE-2009-1336	20		DoS	22/04/2009	10/10/2018	4,9	None	Local	Low	Not required	None	None	Complete	fs/nfs/client.c in the Linux kernel before 2.6.23 does not properly initialize a certain structure member that stores the maximum NFS filename length, which allows local users to cause a denial of service (OOPS) via a long filename, related to the encode_lookup function.
22	CVE-2009-1192				24/04/2009	10/10/2018	4,9	None	Local	Low	Not required	Complete	None	None	The (1) agp_generic_alloc_page and (2) agp_generic_alloc_pages functions in drivers/char/agp/generic.c in the agp subsystem in the Linux kernel before 2.6.30-rc3 do not zero out pages that may later be available to a user-space process, which allows local users to obtain sensitive information by reading these pages.
23	CVE-2009-1184	16		Bypass	05/05/2009	19/03/2012	4,4	None	Local	Medium	Not required	Partial	Partial	Partial	The selinux_ip_postroute_iptables_compat function in security/selinux/hooks.c in the SELinux subsystem in the Linux kernel before 2.6.27.22, and 2.6.28.x before 2.6.28.10, when compat_net is enabled, omits calls to avc_has_perm for the (1) node and (2) port, which allows local users to bypass intended restrictions on network traffic. NOTE: this was incorrectly reported as an issue fixed in 2.6.27.21.
24	CVE-2009-0935	399		DoS	18/03/2009	17/08/2017	4,7	None	Local	Medium	Not required	None	None	Complete	The inotify_read function in the Linux kernel 2.6.27 to 2.6.27.13, 2.6.28 to 2.6.28.2, and 2.6.29-rc3 allows local users to cause a denial of service (OOPS) via a read with an invalid address to an inotify instance, which causes the device's event list mutex to be unlocked twice and prevents proper synchronization of a data structure for the inotify instance.
25	CVE-2009-0676	264			22/02/2009	10/10/2018	2,1	None	Local	Low	Not required	Partial	None	None	The sock_getsockopt function in net/core/sock.c in the Linux kernel before 2.6.28.6 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel memory via an SO_BSDCOMPAT getsockopt request.
26	CVE-2009-0675	264			22/02/2009	10/10/2018	2,1	None	Local	Low	Not required	None	Partial	None	The skfp_ioctl function in drivers/net/skfp/skfddi.c in the Linux kernel before 2.6.28.6 permits SKFP_CLR_STATS requests only when the CAP_NET_ADMIN capability is absent, instead of when this capability is present, which allows local users to reset the driver statistics, related to an "inverted logic" issue.
27	CVE-2009-0605	119		DoS Overflow +Priv Mem. Corr.	17/02/2009	19/03/2012	4,9	None	Local	Low	Not required	None	None	Complete	Stack consumption vulnerability in the do_page_fault function in arch/x86/mm/fault.c in the Linux kernel before 2.6.28.5 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via unspecified vectors that trigger page faults on a machine that has a registered Kprobes probe.
28	CVE-2009-0269	399		DoS Mem. Corr.	26/01/2009	11/10/2018	4,9	None	Local	Low	Not required	None	None	Complete	fs/ecryptfs/inode.c in the eCryptfs subsystem in the Linux kernel before 2.6.28.1 allows local users to cause a denial of service (fault or memory corruption), or possibly have unspecified other impact, via a readlink call that results in an error, leading to use of a -1 return value as an array index.
29	CVE-2009-0065	119		Overflow	07/01/2009	29/09/2017	10	None	Remote	Low	Not required	Complete	Complete	Complete	Buffer overflow in net/sctp/sm_statefuns.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.28-git8 allows remote attackers to have an unknown impact via an FWD-TSN (aka FORWARD-TSN) chunk with a large stream ID.
30	CVE-2009-0031	399		DoS	21/01/2009	29/09/2017	4,9	None	Local	Low	Not required	None	None	Complete	Memory leak in the keyctl_join_session_keyring function (security/keys/keyctl.c) in Linux kernel 2.6.29-rc2 and earlier allows local users to cause a denial of service (kernel memory consumption) via unknown vectors related to a "missing kfree."
31	CVE-2009-0028	264			27/02/2009	11/10/2018	2,1	None	Local	Low	Not required	None	None	Partial	The clone system call in the Linux kernel 2.6.28 and earlier allows local users to send arbitrary signals to a parent process from an unprivileged child process by launching an additional child process with the CLONE_PARENT flag, and then letting this new process exit.
32	CVE-2009-0024	264		DoS +Priv	13/01/2009	19/03/2012	7,2	None	Local	Low	Not required	Complete	Complete	Complete	The sys_remap_file_pages function in mm/fremap.c in the Linux kernel before 2.6.24.1 allows local users to cause a denial of service or gain privileges via unspecified vectors, related to the vm_file structure member, and the mmap_region and do_munmap functions.
33	CVE-2008-6107	399		DoS	10/02/2009	08/08/2017	4,9	None	Local	Low	Not required	None	None	Complete	The (1) sys32_mremap function in arch/sparc64/kernel/sys_sparc32.c, the (2) sparc_mmap_check function in arch/sparc/kernel/sys_sparc.c, and the (3) sparc64_mmap_check function in arch/sparc64/kernel/sys_sparc.c, in the Linux kernel before 2.6.25.4, omit some virtual-address range (aka span) checks when the mremap MREMAP_FIXED bit is not set, which allows local users to cause a denial of service (panic) via unspecified mremap calls, a related issue to CVE-2008-2137.
34	CVE-2008-5713	399		DoS	24/12/2008	03/10/2018	4,9	None	Local	Low	Not required	None	None	Complete	The __qdisc_run function in net/sched/sch_generic.c in the Linux kernel before 2.6.25 on SMP machines allows local users to cause a denial of service (soft lockup) by sending a large amount of network traffic, as demonstrated by multiple simultaneous invocations of the Netperf benchmark application in UDP_STREAM mode.
35	CVE-2008-5702	119		Overflow	22/12/2008	03/10/2018	7,2	None	Local	Low	Not required	Complete	Complete	Complete	Buffer underflow in the ibwdt_ioctl function in drivers/watchdog/ib700wdt.c in the Linux kernel before 2.6.28-rc1 might allow local users to have an unknown impact via a certain /dev/watchdog WDIOC_SETTIMEOUT IOCTL call.
36	CVE-2008-5700	399		DoS	22/12/2008	11/10/2018	1,9	None	Local	Medium	Not required	None	None	Partial	libata in the Linux kernel before 2.6.27.9 does not set minimum timeouts for SG_IO requests, which allows local users to cause a denial of service (Programmed I/O mode on drives) via multiple simultaneous invocations of an unspecified test program.
37	CVE-2008-5182	362			21/11/2008	11/10/2018	6,9	None	Local	Medium	Not required	Complete	Complete	Complete	The inotify functionality in Linux kernel 2.6 before 2.6.28-rc5 might allow local users to gain privileges via unknown vectors related to race conditions in inotify watch removal and umount.

38	CVE-2008-5079	399		DoS	09/12/2008	11/10/2018	4,9	None	Local	Low	Not required	None	None	Complete	net/atm/svc.c in the ATM subsystem in the Linux kernel 2.6.27.8 and earlier allows local users to cause a denial of service (kernel infinite loop) by making two calls to svc_listen for the same socket, and then reading a /proc/net/atm/*vc file, related to corruption of the vcc table.
39	CVE-2008-5029			DoS	10/11/2008	11/10/2018	4,9	None	Local	Low	Not required	None	None	Complete	The __scm_destroy function in net/core/scm.c in the Linux kernel 2.6.27.4, 2.6.26, and earlier makes indirect recursive calls to itself through calls to the fput function, which allows local users to cause a denial of service (panic) via vectors related to sending an SCM_RIGHTS message through a UNIX domain socket and closing file descriptors.
40	CVE-2008-5025	119		DoS Overflow Mem. Corr.	17/11/2008	29/09/2017	7,8	None	Remote	Low	Not required	None	None	Complete	Stack-based buffer overflow in the hfs_cat_find_brec function in fs/hfs/catalog.c in the Linux kernel before 2.6.28-rc1 allows attackers to cause a denial of service (memory corruption or system crash) via an hfs filesystem image with an invalid catalog namelength field, a related issue to CVE-2008-4933.
41	CVE-2008-4933	119		DoS Overflow Mem. Corr.	05/11/2008	29/09/2017	7,8	None	Remote	Low	Not required	None	None	Complete	Buffer overflow in the hfsplus_find_cat function in fs/hfsplus/catalog.c in the Linux kernel before 2.6.28-rc1 allows attackers to cause a denial of service (memory corruption or system crash) via an hfsplus filesystem image with an invalid catalog namelength field, related to the hfsplus_cat_build_key_uni function.
42	CVE-2008-4618	20		DoS	21/10/2008	19/03/2012	7,8	None	Remote	Low	Not required	None	None	Complete	The Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.27 does not properly handle a protocol violation in which a parameter has an invalid length, which allows attackers to cause a denial of service (panic) via unspecified vectors, related to sctp_sf_violation_paramlen, sctp_sf_abort_violation, sctp_make_abort_violation, and incorrect data types in function calls.
43	CVE-2008-4576	287		DoS	15/10/2008	29/09/2017	7,8	None	Remote	Low	Not required	None	None	Complete	sctp in Linux kernel before 2.6.25.18 allows remote attackers to cause a denial of service (OOPS) via an INIT-ACK that states the peer does not support AUTH, which causes the sctp_process_init function to clean up active transports and triggers the OOPS when the T1-Init timer expires.
44	CVE-2008-4554	264		Bypass	15/10/2008	29/09/2017	4,6	None	Local	Low	Not required	Partial	Partial	Partial	The do_splice_from function in fs/splice.c in the Linux kernel before 2.6.27 does not reject file descriptors that have the O_APPEND flag set, which allows local users to bypass append mode and make arbitrary changes to other locations in the file.
45	CVE-2008-4445	200			06/10/2008	30/10/2012	4,7	None	Local	Medium	Not required	Complete	None	None	The sctp_auth_ep_set_hmacs function in net/sctp/auth.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4, when the SCTP-AUTH extension is enabled, does not verify that the identifier index is within the bounds established by SCTP_AUTH_HMAC_ID_MAX, which allows local users to obtain sensitive information via a crafted SCTP_HMAC_IDENT IOCTL request involving the sctp_getsockopt function, a different vulnerability than CVE-200
46	CVE-2008-4395	119		Exec Code Overflow	06/11/2008	08/08/2017	8,3	None	Local Netv	Low	Not required	Complete	Complete	Complete	Multiple buffer overflows in the ndiswrapper module 1.53 for the Linux kernel 2.6 allow remote attackers to execute arbitrary code by sending packets over a local wireless network that specify long ESSIDs.
47	CVE-2008-4307	362		DoS	13/01/2009	11/10/2018	4	None	Local	High	Not required	None	None	Complete	Race condition in the do_setlk function in fs/nfs/file.c in the Linux kernel before 2.6.26 allows local users to cause a denial of service (crash) via vectors resulting in an interrupted RPC call that leads to a stray FL_POSIX lock, related to improper handling of a race between fcntl and close in the EINTR case.
48	CVE-2008-4302	399		DoS	29/09/2008	29/09/2017	4,9	None	Local	Low	Not required	None	None	Complete	fs/splice.c in the splice subsystem in the Linux kernel before 2.6.22.2 does not properly handle a failure of the add_to_page_cache_lru function, and subsequently attempts to unlock a page that was not locked, which allows local users to cause a denial of service (kernel BUG and system crash), as demonstrated by the fio I/O tool.
49	CVE-2008-4210	264			29/09/2008	29/09/2017	4,6	None	Local	Low	Not required	Partial	Partial	Partial	fs/open.c in the Linux kernel before 2.6.22 does not properly strip setuid and setgid bits when there is a write to a file, which allows local users to gain the privileges of a different group, and obtain sensitive information or possibly have unspecified other impact, by creating an executable file in a setgid directory through the (1) truncate or (2) ftruncate function in conjunction with memory-mapped I/O.
50	CVE-2008-4113	200			16/09/2008	11/10/2018	4,7	None	Local	Medium	Not required	Complete	None	None	The sctp_getsockopt_hmac_ident function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4, when the SCTP-AUTH extension is enabled, relies on an untrusted length value to limit copying of data from kernel memory, which allows local users to obtain sensitive information via a crafted SCTP_HMAC_IDENT IOCTL request involving the sctp_getsockopt function.
51	CVE-2008-3833	264			03/10/2008	29/09/2017	4,9	None	Local	Low	Not required	Complete	None	None	The generic_file_splice_write function in fs/splice.c in the Linux kernel before 2.6.19 does not properly strip setuid and setgid bits when there is a write to a file, which allows local users to gain the privileges of a different group, and obtain sensitive information or possibly have unspecified other impact, by splicing into an inode in order to create an executable file in a setgid directory, a different vulnerability than CVE-2008-4210.
52	CVE-2008-3527	264		DoS +Priv	05/11/2008	29/09/2017	4,6	None	Local	Low	Not required	Partial	Partial	Partial	arch/i386/kernel/sysenter.c in the Virtual Dynamic Shared Objects (vDSO) implementation in the Linux kernel before 2.6.21 does not properly check boundaries, which allows local users to gain privileges or cause a denial of service via unspecified vectors, related to the install_special_mapping, syscall, and syscall32_nopage functions.
53	CVE-2007-4567	20		DoS	21/12/2007	03/10/2018	7,8	None	Remote	Low	Not required	None	None	Complete	The ipv6_hop_jumbo function in net/ipv6/exthdrs.c in the Linux kernel before 2.6.22 does not properly validate the hop-by-hop IPv6 extended header, which allows remote attackers to cause a denial of service (NULL pointer dereference and kernel panic) via a crafted IPv6 packet.
54	CVE-2007-3740	264			14/09/2007	29/09/2017	4,4	None	Local	Medium	Not required	Partial	Partial	Partial	The CIFS filesystem in the Linux kernel before 2.6.22, when Unix extension support is enabled, does not honor the umask of a process, which allows local users to gain privileges.

libstdc++

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2019-15847	331			02/09/2019	17/09/2020	5	None	Remote	Low	Not required	Partial	None	None	The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.
2	CVE-2018-12886	209		Overflow Bypass	22/05/2019	24/08/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared agains
3	CVE-2017-11671	338			26/07/2017	12/04/2018	2,1	None	Local	Low	Not required	Partial	None	None	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) version 4.6, 4.7, 4.8, 4.9, 5 before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND and RDSEED intrinsics before it can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to less randomness in random number generation.
4	CVE-2015-5276	200			17/11/2015	12/02/2019	5	None	Remote	Low	Not required	Partial	None	None	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not properly handle short reads from blocking sources, which makes it easier for context-dependent attackers to predict the random values via unspecified vectors.
5	CVE-2008-1685	119		Overflow	06/04/2008	08/08/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	** DISPUTED ** gcc 4.2.0 through 4.3.0 in GNU Compiler Collection, when casts are not used, considers the sum of a pointer and an int to be greater than or equal to the pointer, which might lead to removal of length testing code that was intended as a protection mechanism against integer overflow and buffer overflow attacks, and provide no diagnostic message about this removal. NOTE: the vendor has determined that this compiler behavior is correct according to section 6.5.6 of the C99 s
6	CVE-2008-1367	399		Mem. Corr.	17/03/2008	29/09/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	gcc 4.3.x does not generate a cld instruction while compiling functions used for string manipulation such as memcpy and memmove on x86 and i386, which can prevent the direction flag (DF) from being reset in violation of ABI conventions and cause data to be copied in the wrong direction during signal handling in the Linux kernel, which might allow context-dependent attackers to trigger memory corruption. NOTE: this issue was originally reported for CPU consumption in SBCL.
7	CVE-2006-1902	119		Overflow	20/04/2006	18/10/2018	2,1	None	Local	Low	Not required	None	Partial	None	fold_binary in fold-const.c in GNU Compiler Collection (gcc) 4.1 improperly handles pointer overflow when folding a certain expr comparison to a corresponding offset comparison in cases other than EQ_EXPR and NE_EXPR, which might introduce buffer overflow vulnerabilities into applications that could be exploited by context-dependent attackers.NOTE: the vendor states that the essence of the issue is "not correctly interpreting an offset to a pointer as a signed value."
8	CVE-2002-2439	190		Overflow	23/10/2019	31/10/2019	4,6	None	Local	Low	Not required	Partial	Partial	Partial	Integer overflow in the new[] operator in gcc before 4.8.0 allows attackers to have unspecified impacts.
9	CVE-2000-1219			Overflow	01/11/2000	05/09/2008	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The -ftrapv compiler option in gcc and g++ 3.3.3 and earlier does not handle all types of integer overflows, which may leave applications vulnerable to vulnerabilities related to overflows.

glibc

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2021-38604	476			12/08/2021	07/10/2021	5	None	Remote	Low	Not required	None	None	Partial	In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.
2	CVE-2021-35942	190		DoS	22/07/2021	21/09/2021	6,4	None	Remote	Low	Not required	Partial	None	Partial	The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.
3	CVE-2021-33574	416		DoS	25/05/2021	07/07/2021	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.
4	CVE-2021-27645	415		DoS	24/02/2021	06/07/2021	1,9	None	Local	Medium	Not required	None	None	Partial	The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.
5	CVE-2021-3326	617		DoS	27/01/2021	06/07/2021	5	None	Remote	Low	Not required	None	None	Partial	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
6	CVE-2020-29573	787		Overflow	06/12/2020	26/01/2021	5	None	Remote	Low	Not required	None	None	Partial	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-i
7	CVE-2020-29562	617		DoS	04/12/2020	19/03/2021	2,1	None	Remote	High	???	None	None	Partial	The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
8	CVE-2020-27618	835		DoS	26/02/2021	06/07/2021	2,1	None	Local	Low	Not required	None	None	Partial	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.
9	CVE-2020-10029	119		Overflow	04/03/2020	21/07/2021	2,1	None	Local	Low	Not required	None	None	Partial	The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.
10	CVE-2020-6096	191		Exec Code	01/04/2020	04/03/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, t
11	CVE-2020-1752	416		Exec Code	30/04/2020	29/06/2021	3,7	None	Local	High	Not required	Partial	Partial	Partial	A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.
12	CVE-2020-1751	787		DoS Exec Code	17/04/2020	09/07/2020	5,9	None	Local	Medium	Not required	Partial	Partial	Complete	An out-of-bounds write vulnerability was found in glibc before 2.31 when handling signal trampolines on PowerPC. Specifically, the backtrace function did not properly check the array bounds when storing the frame address, resulting in a denial of service or potential code execution. The highest threat from this vulnerability is to system availability.
13	CVE-2019-101002	330		Bypass	15/07/2019	16/11/2020	5	None	Remote	Low	Not required	Partial	None	None	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability."
14	CVE-2019-101002	200		Bypass +Info	15/07/2019	16/11/2020	5	None	Remote	Low	Not required	Partial	None	None	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
15	CVE-2019-1010023			Exec Code	15/07/2019	16/11/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	** DISPUTED ** GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
16	CVE-2019-101002	119		Overflow Bypass	15/07/2019	10/06/2021	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	** DISPUTED ** GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat."
17	CVE-2019-25013	125			04/01/2021	06/07/2021	7,1	None	Remote	Medium	Not required	None	None	Complete	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
18	CVE-2019-19126	200		Bypass +Info	19/11/2019	21/07/2021	2,1	None	Local	Low	Not required	Partial	None	None	On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.
19	CVE-2019-9192	674			26/02/2019	24/08/2020	5	None	Remote	Low	Not required	None	None	Partial	** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.
20	CVE-2019-9169	125			26/02/2019	09/07/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.
21	CVE-2019-7309				03/02/2019	24/08/2020	2,1	None	Local	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return zero (indicating that the inputs are equal) because the RDX most significant bit is mishandled.
22	CVE-2019-6488	404			18/01/2019	13/06/2020	4,6	None	Local	Low	Not required	Partial	Partial	Partial	The string component in the GNU C Library (aka glibc or libc6) through 2.28, when running on the x32 architecture, incorrectly attempts to use a 64-bit register for size_t in assembly codes, which can lead to a segmentation fault or possibly unspecified other impact, as demonstrated by a crash in __memmove_avx_unaligned_erms in sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S during a memcpy.
23	CVE-2018-100000	787		Exec Code	31/01/2018	03/10/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
24	CVE-2018-20796	674			26/02/2019	05/11/2019	5	None	Remote	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.
25	CVE-2018-19591	20			04/12/2018	09/07/2020	5	None	Remote	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) through 2.28, attempting to resolve a crafted hostname via getaddrinfo() leads to the allocation of a socket descriptor that is not closed. This is related to the if_nametoindex() function.
26	CVE-2018-11237	787		Overflow	18/05/2018	24/08/2020	4,6	None	Local	Low	Not required	Partial	Partial	Partial	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
27	CVE-2018-11236	787		Exec Code Overflow	18/05/2018	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.
28	CVE-2018-6551	787			02/02/2018	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.
29	CVE-2018-6485	787		Overflow	01/02/2018	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
30	CVE-2017-100040	119		Overflow	01/02/2018	04/04/2019	6,9	None	Local	Medium	Not required	Complete	Complete	Complete	A buffer overflow in glibc 2.5 (released on September 29, 2006) and can be triggered through the LD_LIBRARY_PATH environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
31	CVE-2017-100040	772			01/02/2018	03/10/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	A memory leak in glibc 2.1.1 (released on May 24, 1999) can be reached and amplified through the LD_HWCAP_MASK environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
32	CVE-2017-100036	119		Exec Code Overflow	19/06/2017	15/10/2020	7,2	None	Local	Low	Not required	Complete	Complete	Complete	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
33	CVE-2017-17426	190		Overflow	05/12/2017	15/12/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check.
34	CVE-2017-16997	426			18/12/2017	15/10/2020	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileg
35	CVE-2017-15804	119		Overflow	22/10/2017	20/06/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
36	CVE-2017-15671	772		DoS	20/10/2017	03/10/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TILDE, could skip freeing allocated memory when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak).
37	CVE-2017-15670	119		Overflow	20/10/2017	20/06/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
38	CVE-2017-12133	416			07/09/2017	09/07/2020	4,3	None	Remote	Medium	Not required	None	Partial	None	Use-after-free vulnerability in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) before 2.26 allows remote attackers to have unspecified impact via vectors related to error path.
39	CVE-2017-12132	770			01/08/2017	03/10/2019	4,3	None	Remote	Medium	Not required	None	Partial	None	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
40	CVE-2017-8804	502		DoS	07/05/2017	26/08/2020	7,8	None	Remote	Low	Not required	None	None	Complete	** DISPUTED ** The xdr_bytes and xdr_string functions in the GNU C Library (aka glibc or libc6) 2.25 mishandle failures of buffer deserialization, which allows remote attackers to cause a denial of service (virtual memory allocation, or memory consumption if an overcommit setting is not used) via a crafted UDP packet to port 111, a related issue to CVE-2017-8779. NOTE: [Information provided from upstream and references]
41	CVE-2016-10739	20			21/01/2019	06/08/2019	4,6	None	Local	Low	Not required	Partial	Partial	Partial	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
42	CVE-2016-10228	20		DoS	02/03/2017	25/02/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.
43	CVE-2016-6323	284		DoS	07/10/2016	30/10/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
44	CVE-2016-5417	399		DoS	17/02/2017	17/02/2017	5	None	Remote	Low	Not required	None	None	Partial	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.
45	CVE-2016-4429	787		DoS Overflow	10/06/2016	20/07/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	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.
46	CVE-2016-3706	20		DoS Overflow	10/06/2016	29/10/2020	5	None	Remote	Low	Not required	None	None	Partial	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.
47	CVE-2016-3075	119		DoS Overflow	01/06/2016	30/10/2018	5	None	Remote	Low	Not required	None	None	Partial	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.
48	CVE-2016-1234	119		DoS Overflow	01/06/2016	01/09/2021	5	None	Remote	Low	Not required	None	None	Partial	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.
49	CVE-2015-8985	19		DoS	20/03/2017	31/03/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (assertion failure and application crash) via vectors related to extended regular expression processing.
50	CVE-2015-8984	125		DoS	20/03/2017	22/03/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.
51	CVE-2015-8983	190		DoS Exec Code Overflow	20/03/2017	22/03/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a size in bytes, which triggers a heap-based buffer overflow.
52	CVE-2015-8982	190		DoS Exec Code Overflow	15/03/2017	29/06/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
53	CVE-2015-8779	119		DoS Exec Code Overflow	19/04/2016	30/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
54	CVE-2015-8778	119		DoS Exec Code Overflow	19/04/2016	30/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
55	CVE-2015-8777	254		Bypass	20/01/2016	05/01/2018	2,1	None	Local	Low	Not required	None	Partial	None	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.
56	CVE-2015-8776	189		DoS +Info	19/04/2016	30/10/2018	6,4	None	Remote	Low	Not required	Partial	None	Partial	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.
57	CVE-2015-7547	119		DoS Exec Code Overflow	18/02/2016	01/09/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	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.
58	CVE-2015-5277	119		DoS Overflow +Priv	17/12/2015	01/07/2017	7,2	None	Local	Low	Not required	Complete	Complete	Complete	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.
59	CVE-2015-5180	476		DoS	27/06/2017	12/04/2018	5	None	Remote	Low	Not required	None	None	Partial	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).
60	CVE-2015-1781	119		DoS Exec Code Overflow	28/09/2015	17/06/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Buffer overflow in the gethostbyname_r and other unspecified NSS functions in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response, which triggers a call with a misaligned buffer.
61	CVE-2015-1473	119		DoS Overflow	08/04/2015	28/11/2016	6,4	None	Remote	Low	Not required	None	Partial	Partial	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during a risk-management decision for use of the alloca function, which might allow context-dependent attackers to cause a denial of service (segmentation violation) or overwrite memory locations beyond the stack boundary via a long line containing wide characters that are improperly handled in a wscanf call.
62	CVE-2015-1472	119		DoS Overflow	08/04/2015	13/06/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during memory allocation, which allows context-dependent attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long line containing wide characters that are improperly handled in a wscanf call.
63	CVE-2015-0235	787		Exec Code Overflow	28/01/2015	01/09/2021	10	None	Remote	Low	Not required	Complete	Complete	Complete	Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."
64	CVE-2014-9984	119		Exec Code Overflow	12/06/2017	13/06/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	nscd in the GNU C Library (aka glibc or libc6) before version 2.20 does not correctly compute the size of an internal buffer when processing netgroup requests, possibly leading to an nscd daemon crash or code execution as the user running nscd.
65	CVE-2014-9761	119		DoS Exec Code Overflow	19/04/2016	13/06/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	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.
66	CVE-2014-9402	399		DoS	24/02/2015	13/06/2019	7,8	None	Remote	Low	Not required	None	None	Complete	The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS backend in the Name Service Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sending a positive answer while a network name is being process.
67	CVE-2014-8121	17		DoS	27/03/2015	17/10/2018	5	None	Remote	Low	Not required	None	None	Partial	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) 2.21 and earlier does not properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by performing a look-up on a database while iterating over it, which triggers the file pointer to be reset.
68	CVE-2014-7817	20		Exec Code	24/11/2014	30/10/2018	4,6	None	Local	Low	Not required	Partial	Partial	Partial	The wordexp function in GNU C Library (aka glibc) 2.21 does not enforce the WRDE_NOCMD flag, which allows context-dependent attackers to execute arbitrary commands, as demonstrated by input containing "$((`...`))".
69	CVE-2014-6040	119		DoS Overflow	05/12/2014	03/01/2017	5	None	Remote	Low	Not required	None	None	Partial	GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8.
70	CVE-2014-5119	189		DoS Exec Code	29/08/2014	31/03/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Off-by-one error in the __gconv_translit_find function in gconv_trans.c in GNU C Library (aka glibc) allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via vectors related to the CHARSET environment variable and gconv transliteration modules.
71	CVE-2014-4043	94			06/10/2014	13/06/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The posix_spawn_file_actions_addopen function in glibc before 2.20 does not copy its path argument in accordance with the POSIX specification, which allows context-dependent attackers to trigger use-after-free vulnerabilities.
72	CVE-2014-0475	22		Dir. Trav. Bypass	29/07/2014	28/11/2016	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.
73	CVE-2013-7424	17		DoS Exec Code	26/08/2015	28/11/2016	5,1	None	Remote	High	Not required	Partial	Partial	Partial	The getaddrinfo function in glibc before 2.15, when compiled with libidn and the AI_IDN flag is used, allows context-dependent attackers to cause a denial of service (invalid free) and possibly execute arbitrary code via unspecified vectors, as demonstrated by an internationalized domain name to ping6.
74	CVE-2013-7423	17			24/02/2015	01/09/2021	5	None	Remote	Low	Not required	None	Partial	None	The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of requests that trigger a call to the getaddrinfo function.
75	CVE-2013-4788	20		Overflow	04/10/2013	01/07/2017	5,1	None	Remote	High	Not required	Partial	Partial	Partial	The PTR_MANGLE implementation in the GNU C Library (aka glibc or libc6) 2.4, 2.17, and earlier, and Embedded GLIBC (EGLIBC) does not initialize the random value for the pointer guard, which makes it easier for context-dependent attackers to control execution flow by leveraging a buffer-overflow vulnerability in an application and using the known zero value pointer guard to calculate a pointer address.
76	CVE-2013-4458	119		DoS Overflow	12/12/2013	01/07/2017	5	None	Remote	Low	Not required	None	None	Partial	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.18 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers a large number of AF_INET6 address results. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1914.
77	CVE-2013-4412	476			04/11/2019	04/11/2019	5	None	Remote	Low	Not required	None	None	Partial	slim has NULL pointer dereference when using crypt() method from glibc 2.17
78	CVE-2013-4332	189		DoS Overflow	09/10/2013	01/07/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	Multiple integer overflows in malloc/malloc.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allow context-dependent attackers to cause a denial of service (heap corruption) via a large value to the (1) pvalloc, (2) valloc, (3) posix_memalign, (4) memalign, or (5) aligned_alloc functions.
79	CVE-2013-4237	119		DoS Exec Code Overflow	09/10/2013	01/07/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	sysdeps/posix/readdir_r.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted (1) NTFS or (2) CIFS image.
80	CVE-2013-2207	264			09/10/2013	01/07/2017	2,6	None	Local	High	Not required	Partial	Partial	None	pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, which allows local users to change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file system.
81	CVE-2013-1914	119		DoS Overflow	29/04/2013	01/09/2021	5	None	Remote	Low	Not required	None	None	Partial	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.17 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers a large number of domain conversion results.
82	CVE-2013-0242	119		DoS Overflow Mem. Corr.	08/02/2013	29/08/2017	5	None	Remote	Low	Not required	None	None	Partial	Buffer overflow in the extend_buffers function in the regular expression matcher (posix/regexec.c) in glibc, possibly 2.17 and earlier, allows context-dependent attackers to cause a denial of service (memory corruption and crash) via crafted multibyte characters.
83	CVE-2012-6656	20		DoS	05/12/2014	01/07/2017	5	None	Remote	Low	Not required	None	None	Partial	iconvdata/ibm930.c in GNU C Library (aka glibc) before 2.16 allows context-dependent attackers to cause a denial of service (out-of-bounds read) via a multibyte character value of "0xffff" to the iconv function when converting IBM930 encoded data to UTF-8.
84	CVE-2012-4424	119		DoS Exec Code Overflow	09/10/2013	01/07/2017	5,1	None	Remote	High	Not required	Partial	Partial	Partial	Stack-based buffer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string that triggers a malloc failure and use of the alloca function.
85	CVE-2012-4412	189		DoS Exec Code Overflow	09/10/2013	13/06/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Integer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buffer overflow.
86	CVE-2012-3480	189		DoS Exec Code Overflow	25/08/2012	01/07/2017	4,6	None	Local	Low	Not required	Partial	Partial	Partial	Multiple integer overflows in the (1) strtod, (2) strtof, (3) strtold, (4) strtod_l, and other unspecified "related functions" in stdlib in GNU C Library (aka glibc or libc6) 2.16 allow local users to cause a denial of service (application crash) and possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
87	CVE-2012-3406	264		DoS Exec Code Bypass	10/02/2014	22/04/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The vfprintf function in stdio-common/vfprintf.c in GNU C Library (aka glibc) 2.5, 2.12, and probably other versions does not "properly restrict the use of" the alloca function when allocating the SPECS array, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (crash) or possibly execute arbitrary code via a crafted format string using positional parameters and a large number of format specifiers, a differe
88	CVE-2012-3405	189		DoS Bypass	10/02/2014	22/04/2019	5	None	Remote	Low	Not required	None	None	Partial	The vfprintf function in stdio-common/vfprintf.c in libc in GNU C Library (aka glibc) 2.14 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (segmentation fault and crash) via a format string with a large number of format specifiers that triggers "desynchronization within the buffer size handling," a different vulnerability than CVE-2012-3404.
89	CVE-2012-3404	189		DoS Bypass	10/02/2014	22/04/2019	5	None	Remote	Low	Not required	None	None	Partial	The vfprintf function in stdio-common/vfprintf.c in libc in GNU C Library (aka glibc) 2.12 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (stack corruption and crash) via a format string that uses positional parameters and many format specifiers.
90	CVE-2012-0864	189		Overflow Bypass	02/05/2013	03/05/2013	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Integer overflow in the vfprintf function in stdio-common/vfprintf.c in glibc 2.14 and other versions allows context-dependent attackers to bypass the FORTIFY_SOURCE protection mechanism, conduct format string attacks, and write to arbitrary memory via a large number of arguments.
91	CVE-2011-5320	119		DoS Overflow	18/10/2017	08/11/2017	2,1	None	Local	Low	Not required	None	None	Partial	scanf and related functions in glibc before 2.15 allow local users to cause a denial of service (segmentation fault) via a large string of 0s.
92	CVE-2011-4609	399		DoS	02/05/2013	03/05/2013	5	None	Remote	Low	Not required	None	None	Partial	The svc_run function in the RPC implementation in glibc before 2.15 allows remote attackers to cause a denial of service (CPU consumption) via a large number of RPC connections.
93	CVE-2011-2702	94		Exec Code	27/10/2014	31/10/2014	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Integer signedness error in Glibc before 2.13 and eglibc before 2.13, when using Supplemental Streaming SIMD Extensions 3 (SSSE3) optimization, allows context-dependent attackers to execute arbitrary code via a negative length parameter to (1) memcpy-ssse3-rep.S, (2) memcpy-ssse3.S, or (3) memset-sse2.S in sysdeps/i386/i686/multiarch/, which triggers an out-of-bounds read, as demonstrated using the memcpy function.
94	CVE-2011-1659	189		DoS Overflow	08/04/2011	09/10/2018	5	None	Remote	Low	Not required	None	None	Partial	Integer overflow in posix/fnmatch.c in the GNU C Library (aka glibc or libc6) 2.13 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long UTF8 string that is used in an fnmatch call with a crafted pattern argument, a different vulnerability than CVE-2011-1071.
95	CVE-2011-1658	264			08/04/2011	09/10/2018	3,7	None	Local	High	Not required	Partial	Partial	Partial	ld.so in the GNU C Library (aka glibc or libc6) 2.13 and earlier expands the $ORIGIN dynamic string token when RPATH is composed entirely of this token, which might allow local users to gain privileges by creating a hard link in an arbitrary directory to a (1) setuid or (2) setgid program with this RPATH value, and then executing the program with a crafted value for the LD_PRELOAD environment variable, a different vulnerability than CVE-2010-3847 and CVE-2011-0536. NOTE: it is not expe
96	CVE-2011-1095	264			10/04/2011	09/10/2018	6,2	None	Local	High	Not required	Complete	Complete	Complete	locale/programs/locale.c in locale in the GNU C Library (aka glibc or libc6) before 2.13 does not quote its output, which might allow local users to gain privileges via a crafted localization environment variable, in conjunction with a program that executes a script that uses the eval function.
97	CVE-2011-1089	16			10/04/2011	07/12/2016	3,3	None	Local	Medium	Not required	Partial	Partial	None	The addmntent function in the GNU C Library (aka glibc or libc6) 2.13 and earlier does not report an error status for failed attempts to write to the /etc/mtab file, which makes it easier for local users to trigger corruption of this file, as demonstrated by writes from a process with a small RLIMIT_FSIZE value, a different vulnerability than CVE-2010-0296.
98	CVE-2011-1071	399		DoS Exec Code	08/04/2011	09/10/2018	5,1	None	Remote	High	Not required	Partial	Partial	Partial	The GNU C Library (aka glibc or libc6) before 2.12.2 and Embedded GLIBC (EGLIBC) allow context-dependent attackers to execute arbitrary code or cause a denial of service (memory consumption) via a long UTF8 string that is used in an fnmatch call, aka a "stack extension attack," a related issue to CVE-2010-2898, CVE-2010-1917, and CVE-2007-4782, as originally reported for use of this library by Google Chrome.
99	CVE-2010-4756	399		DoS	02/03/2011	01/09/2021	4	None	Remote	Low	???	None	None	Partial	The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.
100	CVE-2010-4052	399	1	DoS	13/01/2011	10/10/2018	5	None	Remote	Low	Not required	None	None	Partial	Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD.
101	CVE-2010-4051		1	DoS Overflow Bypass	13/01/2011	18/06/2021	5	None	Remote	Low	Not required	None	None	Partial	The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a "RE_DUP_MAX overflow."
102	CVE-2010-3856	264			07/01/2011	13/06/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	ld.so in the GNU C Library (aka glibc or libc6) before 2.11.3, and 2.12.x before 2.12.2, does not properly restrict use of the LD_AUDIT environment variable to reference dynamic shared objects (DSOs) as audit objects, which allows local users to gain privileges by leveraging an unsafe DSO located in a trusted library directory, as demonstrated by libpcprofile.so.

103	CVE-2010-3847	59			07/01/2011	10/10/2018	6,9	None	Local	Medium	Not required	Complete	Complete	Complete	elf/dl-load.c in ld.so in the GNU C Library (aka glibc or libc6) through 2.11.2, and 2.12.x through 2.12.1, does not properly handle a value of $ORIGIN for the LD_AUDIT environment variable, which allows local users to gain privileges via a crafted dynamic shared object (DSO) located in an arbitrary directory.
104	CVE-2010-3192	200		Overflow +Info	14/10/2010	31/03/2020	5	None	Remote	Low	Not required	Partial	None	None	Certain run-time memory protection mechanisms in the GNU C Library (aka glibc or libc6) print argv[0] and backtrace information, which might allow context-dependent attackers to obtain sensitive information from process memory by executing an incorrect program, as demonstrated by a setuid program that contains a stack-based buffer overflow error, related to the __fortify_fail function in debug/fortify_fail.c, and the __stack_chk_fail (aka stack protection) and __chk_fail (aka FORTIFY_SOU
105	CVE-2010-0830	189		Exec Code	01/06/2010	17/08/2017	5,1	None	Remote	High	Not required	Partial	Partial	Partial	Integer signedness error in the elf_get_dynamic_info function in elf/dynamic-link.h in ld.so in the GNU C Library (aka glibc or libc6) 2.0.1 through 2.11.1, when the --verify option is used, allows user-assisted remote attackers to execute arbitrary code via a crafted ELF program with a negative value for a certain d_tag structure member in the ELF header.
106	CVE-2010-0296	20		DoS +Priv	01/06/2010	13/06/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	The encode_name macro in misc/mntent_r.c in the GNU C Library (aka glibc or libc6) 2.11.1 and earlier, as used by ncpmount and mount.cifs, does not properly handle newline characters in mountpoint names, which allows local users to cause a denial of service (mtab corruption), or possibly modify mount options and gain privileges, via a crafted mount request.
107	CVE-2010-0015	255			14/01/2010	07/12/2016	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	nis/nss_nis/nis-pwd.c in the GNU C Library (aka glibc or libc6) 2.7 and Embedded GLIBC (EGLIBC) 2.10.2 adds information from the passwd.adjunct.byname map to entries in the passwd map, which allows remote attackers to obtain the encrypted passwords of NIS accounts by calling the getpwnam function.
108	CVE-2009-5155	19		DoS	26/02/2019	29/06/2021	5	None	Remote	Low	Not required	None	None	Partial	In the GNU C Library (aka glibc or libc6) before 2.28, parse_reg_exp in posix/regcomp.c misparses alternatives, which allows attackers to cause a denial of service (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression match.
109	CVE-2009-5064	264			30/03/2011	19/01/2012	6,9	None	Local	Medium	Not required	Complete	Complete	Complete	** DISPUTED ** ldd in the GNU C Library (aka glibc or libc6) 2.13 and earlier allows local users to gain privileges via a Trojan horse executable file linked with a modified loader that omits certain LD_TRACE_LOADED_OBJECTS checks. NOTE: the GNU C Library vendor states "This is just nonsense. There are a gazillion other ways to introduce code if people are downloading arbitrary binaries and install them in appropriate directories or set LD_LIBRARY_PATH etc."
110	CVE-2009-5029	189		DoS Exec Code Overflow	02/05/2013	03/05/2013	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Integer overflow in the __tzfile_read function in glibc before 2.15 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted timezone (TZ) file, as demonstrated using vsftpd.
111	CVE-2009-4881	189		DoS Overflow	01/06/2010	17/08/2017	5	None	Remote	Low	Not required	None	None	Partial	Integer overflow in the __vstrfmon_l function in stdlib/strfmon_l.c in the strfmon implementation in the GNU C Library (aka glibc or libc6) before 2.10.1 allows context-dependent attackers to cause a denial of service (application crash) via a crafted format string, as demonstrated by the %99999999999999999999n string, a related issue to CVE-2008-1391.
112	CVE-2009-4880	189		DoS Overflow	01/06/2010	17/08/2017	5	None	Remote	Low	Not required	None	None	Partial	Multiple integer overflows in the strfmon implementation in the GNU C Library (aka glibc or libc6) 2.10.1 and earlier allow context-dependent attackers to cause a denial of service (memory consumption or application crash) via a crafted format string, as demonstrated by a crafted first argument to the money_format function in PHP, a related issue to CVE-2008-1391.
113	CVE-2006-7254	19		DoS	10/04/2019	11/04/2019	2,1	None	Local	Low	Not required	None	None	Partial	The nscd daemon in the GNU C Library (glibc) before version 2.5 does not close incoming client sockets if they cannot be handled by the daemon, allowing local users to carry out a denial of service attack on the daemon.
114	CVE-2005-3590	119		Overflow	10/04/2019	11/04/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The getgrouplist function in the GNU C library (glibc) before version 2.3.5, when invoked with a zero argument, writes to the passed pointer even if the specified array size is zero, leading to a buffer overflow and potentially allowing attackers to corrupt memory.
115	CVE-2004-1453				31/12/2004	11/10/2017	2,1	None	Local	Low	Not required	Partial	None	None	GNU glibc 2.3.4 before 2.3.4.20040619, 2.3.3 before 2.3.3.20040420, and 2.3.2 before 2.3.2-r10 does not restrict the use of LD_DEBUG for a setuid program, which allows local users to gain sensitive information, such as the list of symbols used by the program.
116	CVE-2004-1382				31/12/2004	18/10/2016	2,1	None	Local	Low	Not required	None	Partial	None	The glibcbug script in glibc 2.3.4 and earlier allows local users to overwrite arbitrary files via a symlink attack on temporary files, a different vulnerability than CVE-2004-0968.
117	CVE-2004-0968				09/02/2005	11/10/2017	2,1	None	Local	Low	Not required	None	Partial	None	The catchsegv script in glibc 2.3.2 and earlier allows local users to overwrite files via a symlink attack on temporary files.
118	CVE-2003-0859			DoS	15/12/2003	11/10/2017	4,9	None	Local	Low	Not required	None	None	Complete	The getifaddrs function in GNU libc (glibc) 2.2.4 and earlier allows local users to cause a denial of service by sending spoofed messages as other users to the kernel netlink interface.
119	CVE-2003-0028			Exec Code Overflow	25/03/2003	21/01/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Integer overflow in the xdrmem_getbytes() function, and possibly other functions, of XDR (external data representation) libraries derived from SunRPC, including libnsl, libc, glibc, and dietlibc, allows remote attackers to execute arbitrary code via certain integer values in length fields, a different vulnerability than CVE-2002-0391.
120	CVE-2002-1265			DoS	12/11/2002	10/10/2017	5	None	Remote	Low	Not required	None	None	Partial	The Sun RPC functionality in multiple libc implementations does not provide a time-out mechanism when reading data from TCP connections, which allows remote attackers to cause a denial of service (hang).
121	CVE-2002-1146			DoS Overflow	11/10/2002	10/09/2008	5	None	Remote	Low	Not required	None	None	Partial	The BIND 4 and BIND 8.2.x stub resolver libraries, and other libraries such as glibc 2.2.5 and earlier, libc, and libresolv, use the maximum buffer size instead of the actual size when processing a DNS response, which causes the stub resolvers to read past the actual boundary ("read buffer overflow"), allowing remote attackers to cause a denial of service (crash).
122	CVE-2002-0684			Exec Code Overflow	12/08/2002	18/10/2016	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflow in DNS resolver functions that perform lookup of network names and addresses, as used in BIND 4.9.8 and ported to glibc 2.2.5 and earlier, allows remote malicious DNS servers to execute arbitrary code through a subroutine used by functions such as getnetbyname and getnetbyaddr.
123	CVE-2000-0959				19/12/2000	10/10/2017	1,2	None	Local	High	Not required	None	Partial	None	glibc2 does not properly clear the LD_DEBUG_OUTPUT and LD_DEBUG environmental variables when a program is spawned from a setuid program, which could allow local users to overwrite files via a symlink attack.
124	CVE-2000-0824			Exec Code	14/11/2000	10/10/2017	7,2	None	Local	Low	Not required	Complete	Complete	Complete	The unsetenv function in glibc 2.1.1 does not properly unset an environmental variable if the variable is provided twice to a program, which could allow local users to execute arbitrary commands in setuid programs by specifying their own duplicate environmental variables such as LD_PRELOAD or LD_LIBRARY_PATH.
125	CVE-2000-0335				03/05/2000	10/09/2008	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	The resolver in glibc 2.1.3 uses predictable IDs, which allows a local attacker to spoof DNS query results.
126	CVE-1999-0199	252			06/10/2020	03/12/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	manual/search.texi in the GNU C Library (aka glibc) before 2.2 lacks a statement about the unspecified tdelete return value upon deletion of a tree's root, which might allow attackers to access a dangling pointer in an application whose developer was unaware of a documentation update from 1999.

X11

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2013-4396	399		DoS Exec Code	10/10/2013	28/11/2016	6,5	None	Remote	Low	???	Partial	Partial	Partial	Use-after-free vulnerability in the doImageText function in dix/dixfonts.c in the xorg-server module before 1.14.4 in X.Org X11 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted ImageText request that triggers memory-allocation failure.
2	CVE-2012-1699	119		DoS Overflow Mem. Corr. +Info	21/12/2012	19/09/2017	3,6	None	Local	Low	Not required	Partial	None	Partial	The ProcSetEventMask function in difs/events.c in the xfs font server for X.Org X11R6 through X11R6.6 and XFree86 before 3.3.3 calls the SendErrToClient function with a mask value instead of a pointer, which allows local users to cause a denial of service (memory corruption and crash) or obtain potentially sensitive information from memory via a SetEventMask request that triggers an invalid pointer dereference.
3	CVE-2012-0064	264		Bypass	10/02/2014	11/02/2014	4,6	None	Local	Low	Not required	Partial	Partial	Partial	xkeyboard-config before 2.5 in X.Org before 7.6 enables certain XKB debugging functions by default, which allows physically proximate attackers to bypass an X screen lock via keyboard combinations that break the input grab.

libncurses

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2021-39537	787		Overflow	20/09/2021	18/10/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	An issue was discovered in ncurses through v6.2-1. _nc_captoinfo in captoinfo.c has a heap-based buffer overflow.
2	CVE-2019-17595	125			14/10/2019	08/02/2021	5,8	None	Remote	Medium	Not required	Partial	None	Partial	There is a heap-based buffer over-read in the fmt_entry function in tinfo/comp_hash.c in the terminfo library in ncurses before 6.1-20191012.
3	CVE-2019-17594	125			14/10/2019	10/02/2021	4,6	None	Local	Low	Not required	Partial	Partial	Partial	There is a heap-based buffer over-read in the _nc_find_entry function in tinfo/comp_hash.c in the terminfo library in ncurses before 6.1-20191012.
4	CVE-2018-19217	476		DoS	12/11/2018	18/04/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	** DISPUTED ** In ncurses, possibly a 6.x version, there is a NULL pointer dereference at the function _nc_name_match that will lead to a denial of service attack. NOTE: the original report stated version 6.1, but the issue did not reproduce for that version according to the maintainer or a reliable third-party.
5	CVE-2018-19211	476		DoS	12/11/2018	23/04/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	In ncurses 6.1, there is a NULL pointer dereference at function _nc_parse_entry in parse_entry.c that will lead to a denial of service attack. The product proceeds to the dereference code path even after a "dubious character `*' in name or alias field" detection.
6	CVE-2017-16879	787		DoS Exec Code Overflow	22/11/2017	29/06/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Stack-based buffer overflow in the _nc_write_entry function in tinfo/write_entry.c in ncurses 6.0 allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted terminfo file, as demonstrated by tic.
7	CVE-2017-13734	119		DoS Overflow	29/08/2017	21/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an illegal address access in the _nc_safe_strcat function in strings.c in ncurses 6.0 that will lead to a remote denial of service attack.
8	CVE-2017-13733	119		DoS Overflow	29/08/2017	29/06/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an illegal address access in the fmt_entry function in progs/dump_entry.c in ncurses 6.0 that might lead to a remote denial of service attack.
9	CVE-2017-13732	119		DoS Overflow	29/08/2017	29/06/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an illegal address access in the function dump_uses() in progs/dump_entry.c in ncurses 6.0 that might lead to a remote denial of service attack.
10	CVE-2017-13731	119		DoS Overflow	29/08/2017	29/06/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an illegal address access in the function postprocess_termcap() in parse_entry.c in ncurses 6.0 that will lead to a remote denial of service attack.
11	CVE-2017-13730	119		DoS Overflow	29/08/2017	29/06/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an illegal address access in the function _nc_read_entry_source() in progs/tic.c in ncurses 6.0 that might lead to a remote denial of service attack.
12	CVE-2017-13729	119		DoS Overflow	29/08/2017	29/06/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an illegal address access in the _nc_save_str function in alloc_entry.c in ncurses 6.0. It will lead to a remote denial of service attack.
13	CVE-2017-13728	835		DoS	29/08/2017	29/06/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	There is an infinite loop in the next_char function in comp_scan.c in ncurses 6.0, related to libtic. A crafted input will lead to a remote denial of service attack.
14	CVE-2017-11113	476		DoS	08/07/2017	06/05/2019	5	None	Remote	Low	Not required	None	None	Partial	In ncurses 6.0, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.
15	CVE-2017-11112	20		DoS	08/07/2017	21/10/2018	5	None	Remote	Low	Not required	None	None	Partial	In ncurses 6.0, there is an attempted 0xffffffffffffffff access in the append_acs function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.
16	CVE-2017-10685	134		Exec Code	29/06/2017	03/10/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	In ncurses 6.0, there is a format string vulnerability in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack.
17	CVE-2017-10684	119		Exec Code Overflow	29/06/2017	29/06/2021	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack.

libpng

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2020-27818	125		DoS	08/12/2020	08/12/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	A flaw was found in the check_chunk_name() function of pngcheck-2.4.0. An attacker able to pass a malicious file to be processed by pngcheck could cause a temporary denial of service, posing a low risk to application availability.
2	CVE-2019-7317	416			04/02/2019	20/10/2021	2,6	None	Remote	High	Not required	None	None	Partial	png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.
3	CVE-2019-6129	401			11/01/2019	24/08/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	** DISPUTED ** png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp. NOTE: a third party has stated "I don't think it is libpng's job to free this buffer."
4	CVE-2018-14550	787		Overflow	10/07/2019	20/10/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	An issue has been found in third-party PNM decoding associated with libpng 1.6.35. It is a stack-based buffer overflow in the function get_token in pnm2png.c in pnm2png.
5	CVE-2018-14048				13/07/2018	08/09/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	An issue has been found in libpng 1.6.34. It is a SEGV in the function png_free_data in png.c, related to the recommended error handling for png_read_image.
6	CVE-2018-13785	369		DoS Overflow	09/07/2018	08/09/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngrutil.c) may trigger an integer overflow and resultant divide-by-zero while processing a crafted PNG file, leading to a denial of service.
7	CVE-2017-12652	20			10/07/2019	17/09/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	libpng before 1.6.32 does not properly check the length of chunks against the user limit.
8	CVE-2016-10087	476			30/01/2017	29/06/2021	5	None	Remote	Low	Not required	None	None	Partial	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into a png structure, removing the text, and then adding another text chunk to the structure.
9	CVE-2016-3751				11/07/2016	11/07/2016	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Unspecified vulnerability in libpng before 1.6.20, as used in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01, allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 23265085.
10	CVE-2015-8540	189			14/04/2016	29/06/2021	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	Integer underflow in the png_check_keyword function in pngwutil.c in libpng 0.90 through 0.99, 1.0.x before 1.0.66, 1.1.x and 1.2.x before 1.2.56, 1.3.x and 1.4.x before 1.4.19, and 1.5.x before 1.5.26 allows remote attackers to have unspecified impact via a space character as a keyword in a PNG image, which triggers an out-of-bounds read.
11	CVE-2015-8472	119		DoS Overflow	21/01/2016	04/11/2017	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflow in the png_set_PLTE function in libpng before 1.0.65, 1.1.x and 1.2.x before 1.2.55, 1.3.x, 1.4.x before 1.4.18, 1.5.x before 1.5.25, and 1.6.x before 1.6.20 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8126.
12	CVE-2015-8126	120		DoS Overflow	13/11/2015	31/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng before 1.0.64, 1.1.x and 1.2.x before 1.2.54, 1.3.x and 1.4.x before 1.4.17, 1.5.x before 1.5.24, and 1.6.x before 1.6.19 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.
13	CVE-2015-7981	200			24/11/2015	01/07/2017	5	None	Remote	Low	Not required	Partial	None	None	The png_convert_to_rfc1123 function in png.c in libpng 1.0.x before 1.0.64, 1.2.x before 1.2.54, and 1.4.x before 1.4.17 allows remote attackers to obtain sensitive process memory information via crafted tIME chunk data in an image file, which triggers an out-of-bounds read.
14	CVE-2015-0973	119		Exec Code Overflow	18/01/2015	20/10/2016	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflow in the png_read_IDAT_data function in pngrutil.c in libpng before 1.5.21 and 1.6.x before 1.6.16 allows context-dependent attackers to execute arbitrary code via IDAT data with a large width, a different vulnerability than CVE-2014-9495.
15	CVE-2014-9495	119		Exec Code Overflow	10/01/2015	18/10/2016	10	None	Remote	Low	Not required	Complete	Complete	Complete	Heap-based buffer overflow in the png_combine_row function in libpng before 1.5.21 and 1.6.x before 1.6.16, when running on 64-bit systems, might allow context-dependent attackers to execute arbitrary code via a "very wide interlaced" PNG image.
16	CVE-2014-0333	189		DoS	27/02/2014	26/03/2014	5	None	Remote	Low	Not required	None	None	Partial	The png_push_read_chunk function in pngpread.c in the progressive decoder in libpng 1.6.x through 1.6.9 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via an IDAT chunk with a length of zero.
17	CVE-2013-7354	189		DoS Overflow	06/05/2014	31/12/2016	5	None	Remote	Low	Not required	None	None	Partial	Multiple integer overflows in libpng before 1.5.14rc03 allow remote attackers to cause a denial of service (crash) via a crafted image to the (1) png_set_sPLT or (2) png_set_text_2 function, which triggers a heap-based buffer overflow.
18	CVE-2013-7353	189		DoS Overflow	06/05/2014	31/12/2016	5	None	Remote	Low	Not required	None	None	Partial	Integer overflow in the png_set_unknown_chunks function in libpng/pngset.c in libpng before 1.5.14beta08 allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a crafted image, which triggers a heap-based buffer overflow.
19	CVE-2013-6954			DoS	12/01/2014	05/01/2018	5	None	Remote	Low	Not required	None	None	Partial	The png_do_expand_palette function in libpng before 1.6.8 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via (1) a PLTE chunk of zero bytes or (2) a NULL palette, related to pngrtran.c and pngset.c.
20	CVE-2012-3425	119		DoS Overflow	13/08/2012	30/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	The png_push_read_zTXt function in pngpread.c in libpng 1.0.x before 1.0.58, 1.2.x before 1.2.48, 1.4.x before 1.4.10, and 1.5.x before 1.5.10 allows remote attackers to cause a denial of service (out-of-bounds read) via a large avail_in field value in a PNG image.
21	CVE-2011-3464	189		DoS Exec Code Overflow	22/07/2012	23/07/2012	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Off-by-one error in the png_formatted_warning function in pngerror.c in libpng 1.5.4 through 1.5.7 might allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unspecified vectors, which trigger a stack-based buffer overflow.
22	CVE-2011-3048	119		DoS Exec Code Overflow	29/05/2012	29/12/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The png_set_text_2 function in pngset.c in libpng 1.0.x before 1.0.59, 1.2.x before 1.2.49, 1.4.x before 1.4.11, and 1.5.x before 1.5.10 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted text chunk in a PNG image file, which triggers a memory allocation failure that is not properly handled, leading to a heap-based buffer overflow.
23	CVE-2011-3045	190		DoS Exec Code	22/03/2012	14/04/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Integer signedness error in the png_inflate function in pngrutil.c in libpng before 1.4.10beta01, as used in Google Chrome before 17.0.963.83 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file, a different vulnerability than CVE-2011-3026.
24	CVE-2011-2692	119		DoS Overflow Mem. Corr.	17/07/2011	06/08/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The png_handle_sCAL function in pngrutil.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4 does not properly handle invalid sCAL chunks, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a crafted PNG image that triggers the reading of uninitialized memory.
25	CVE-2011-2691	476		DoS	17/07/2011	06/08/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	The png_err function in pngerror.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4 makes a function call using a NULL pointer argument instead of an empty-string argument, which allows remote attackers to cause a denial of service (application crash) via a crafted PNG image.
26	CVE-2011-2690	120		Overflow	17/07/2011	06/08/2020	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Buffer overflow in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4, when used by an application that calls the png_rgb_to_gray function but not the png_set_expand function, allows remote attackers to overwrite memory with an arbitrary amount of data, and possibly have unspecified other impact, via a crafted PNG image.
27	CVE-2011-2501	125		DoS	17/07/2011	06/08/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	The png_format_buffer function in pngerror.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4 allows remote attackers to cause a denial of service (application crash) via a crafted PNG image that triggers an out-of-bounds read during the copying of error-message data. NOTE: this vulnerability exists because of a CVE-2004-0421 regression. NOTE: this is called an off-by-one error by some sources.
28	CVE-2011-0408	119		DoS Exec Code Overflow	18/01/2011	17/08/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	pngrtran.c in libpng 1.5.x before 1.5.1 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted palette-based PNG image that triggers a buffer overflow, related to the png_do_expand_palette function, the png_do_rgb_to_gray function, and an integer underflow. NOTE: some of these details are obtained from third party information.
29	CVE-2010-2249	401		DoS	30/06/2010	14/08/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	Memory leak in pngrutil.c in libpng before 1.2.44, and 1.4.x before 1.4.3, allows remote attackers to cause a denial of service (memory consumption and application crash) via a PNG image containing malformed Physical Scale (aka sCAL) chunks.
30	CVE-2010-1205	120		Exec Code Overflow	30/06/2010	14/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Buffer overflow in pngpread.c in libpng before 1.2.44 and 1.4.x before 1.4.3, as used in progressive applications, might allow remote attackers to execute arbitrary code via a PNG image that triggers an additional data row.
31	CVE-2010-0205	400		DoS	03/03/2010	07/08/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	The png_decompress_chunk function in pngrutil.c in libpng 1.0.x before 1.0.53, 1.2.x before 1.2.43, and 1.4.x before 1.4.1 does not properly handle compressed ancillary-chunk data that has a disproportionately large uncompressed representation, which allows remote attackers to cause a denial of service (memory and CPU consumption, and application hang) via a crafted PNG file, as demonstrated by use of the deflate compression method on data composed of many occurrences of the sa
32	CVE-2009-5063	401		DoS	31/08/2011	09/09/2020	5	None	Remote	Low	Not required	None	None	Partial	Memory leak in the embedded_profile_len function in pngwutil.c in libpng before 1.2.39beta5 allows context-dependent attackers to cause a denial of service (memory leak or segmentation fault) via a JPEG image containing an iCCP chunk with a negative embedded profile length. NOTE: this is due to an incomplete fix for CVE-2006-7244.
33	CVE-2009-2042	200			12/06/2009	17/08/2017	4,3	None	Remote	Medium	Not required	Partial	None	None	libpng before 1.2.37 does not properly parse 1-bit interlaced images with width values that are not divisible by 8, which causes libpng to include uninitialized bits in certain rows of a PNG file and might allow remote attackers to read portions of sensitive memory via "out-of-bounds pixels" in the file.
34	CVE-2009-0040	94		DoS Exec Code	22/02/2009	11/10/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png_read_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.
35	CVE-2008-6218	399		DoS	20/02/2009	11/10/2018	7,1	None	Remote	Medium	Not required	None	None	Complete	Memory leak in the png_handle_tEXt function in pngrutil.c in libpng before 1.2.33 rc02 and 1.4.0 beta36 allows context-dependent attackers to cause a denial of service (memory exhaustion) via a crafted PNG file.
36	CVE-2008-5907				15/01/2009	08/11/2018	5	None	Remote	Low	Not required	None	Partial	None	The png_check_keyword function in pngwutil.c in libpng before 1.0.42, and 1.2.x before 1.2.34, might allow context-dependent attackers to set the value of an arbitrary memory location to zero via vectors involving creation of crafted PNG files with keywords, related to an implicit cast of the '\0' character constant to a NULL pointer. NOTE: some sources incorrectly report this as a double free vulnerability.
37	CVE-2008-3964	399		DoS	11/09/2008	08/08/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	Multiple off-by-one errors in libpng before 1.2.32beta01, and 1.4 before 1.4.0beta34, allow context-dependent attackers to cause a denial of service (crash) or have unspecified other impact via a PNG image with crafted zTXt chunks, related to (1) the png_push_read_zTXt function in pngread.c, and possibly related to (2) pngtest.c.
38	CVE-2008-1382	189		DoS Exec Code	14/04/2008	11/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	libpng 1.0.6 through 1.0.32, 1.2.0 through 1.2.26, and 1.4.0beta01 through 1.4.0beta19 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a PNG file with zero length "unknown" chunks, which trigger an access of uninitialized memory.
39	CVE-2007-5269	20		DoS	08/10/2007	15/10/2018	5	None	Remote	Low	Not required	None	None	Partial	Certain chunk handlers in libpng before 1.0.29 and 1.2.x before 1.2.21 allow remote attackers to cause a denial of service (crash) via crafted (1) pCAL (png_handle_pCAL), (2) sCAL (png_handle_sCAL), (3) tEXt (png_push_read_tEXt), (4) iTXt (png_handle_iTXt), and (5) ztXT (png_handle_ztXt) chunking in PNG images, which trigger out-of-bounds read operations.
40	CVE-2007-5268			DoS	08/10/2007	26/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	pngrtran.c in libpng before 1.0.29 and 1.2.x before 1.2.21 use (1) logical instead of bitwise operations and (2) incorrect comparisons, which might allow remote attackers to cause a denial of service (crash) via a crafted PNG image.
41	CVE-2007-5267	189		DoS	08/10/2007	15/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	Off-by-one error in ICC profile chunk handling in the png_set_iCCP function in pngset.c in libpng before 1.2.22 beta1 allows remote attackers to cause a denial of service (crash) via a crafted PNG image, due to an incorrect fix for CVE-2007-5266.
42	CVE-2007-5266	189		DoS	08/10/2007	26/10/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	Off-by-one error in ICC profile chunk handling in the png_set_iCCP function in pngset.c in libpng before 1.0.29 beta1 and 1.2.x before 1.2.21 beta1 allows remote attackers to cause a denial of service (crash) via a crafted PNG image that prevents a name field from being NULL terminated.
43	CVE-2006-7244	399		DoS	31/08/2011	15/06/2012	5	None	Remote	Low	Not required	None	None	Partial	Memory leak in pngwutil.c in libpng 1.2.13beta1, and other versions before 1.2.15beta3, allows context-dependent attackers to cause a denial of service (memory leak or segmentation fault) via a JPEG image containing an iCCP chunk with a negative embedded profile length.

libjpeg

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2020-14153	125			15/06/2020	11/08/2020	5,8	None	Remote	Medium	Not required	Partial	None	Partial	In IJG JPEG (aka libjpeg) from version 8 through 9c, jdhuff.c has an out-of-bounds array read for certain table pointers.
2	CVE-2020-14152	400			15/06/2020	31/07/2020	5,8	None	Remote	Medium	Not required	Partial	None	Partial	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnobs.c in djpeg does not honor the max_memory_to_use setting, possibly causing excessive memory consumption.
3	CVE-2018-11813	834			06/06/2018	25/06/2020	5	None	Remote	Low	Not required	None	None	Partial	libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.
4	CVE-2018-11214			DoS	16/05/2018	03/10/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
5	CVE-2018-11213			DoS	16/05/2018	03/10/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
6	CVE-2018-11212	369		DoS	16/05/2018	07/01/2021	4,3	None	Remote	Medium	Not required	None	None	Partial	An issue was discovered in libjpeg 9a and 9d. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file.

libopencv

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2019-19624	125			06/12/2019	17/12/2019	6,4	None	Remote	Low	Not required	Partial	None	Partial	An out-of-bounds read was discovered in OpenCV before 4.1.1. Specifically, variable coarsest_scale is assumed to be greater than or equal to finest_scale within the calc()/ocl_calc() functions in dis_flow.cpp. However, this is not true when dealing with small images, leading to an out-of-bounds read of the heap-allocated arrays Ux and Uy.
2	CVE-2019-16249	125			11/09/2019	03/12/2019	5	None	Remote	Low	Not required	Partial	None	None	OpenCV 4.1.1 has an out-of-bounds read in hal_baseline::v_load in core/hal/intrin_sse.hpp when called from computeSSDMeanNorm in modules/video/src/dis_flow.cpp.
3	CVE-2019-15939	369			05/09/2019	09/01/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	An issue was discovered in OpenCV 4.1.0. There is a divide-by-zero error in cv::HOGDescriptor::getDescriptorSize in modules/objdetect/src/hog.cpp.
4	CVE-2019-14493	476			01/08/2019	05/08/2019	5	None	Remote	Low	Not required	None	None	Partial	An issue was discovered in OpenCV before 4.1.1. There is a NULL pointer dereference in the function cv::XMLParser::parse at modules/core/src/persistence.cpp.
5	CVE-2019-14492	125		DoS	01/08/2019	17/04/2020	5	None	Remote	Low	Not required	None	None	Partial	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read/write in the function HaarEvaluator::OptFeature::calc in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.
6	CVE-2019-14491	125		DoS	01/08/2019	02/12/2019	6,4	None	Remote	Low	Not required	Partial	None	Partial	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read in the function cv::predictOrdered<cv::HaarEvaluator> in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.
7	CVE-2019-5064	120		Exec Code Overflow	03/01/2020	21/07/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV, before version 4.2.0. A specially crafted JSON file can cause a buffer overflow, resulting in multiple heap corruptions and potentially code execution. An attacker can provide a specially crafted file to trigger this vulnerability.
8	CVE-2019-5063	120		Exec Code Overflow	03/01/2020	21/07/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV 4.1.0. A specially crafted XML file can cause a buffer overflow, resulting in multiple heap corruptions and potential code execution. An attacker can provide a specially crafted file to trigger this vulnerability.
9	CVE-2018-7714	617		DoS	05/03/2018	10/02/2020	5	None	Remote	Low	Not required	None	None	Partial	** DISPUTED ** The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (pixels <= (1<<30)) may be false. Note: "OpenCV CV_Assert is not an assertion (C-like assert()), it is regular C++ exception which can raised in case of invalid or non-supported parameters."
10	CVE-2018-7713	617		DoS	05/03/2018	10/02/2020	5	None	Remote	Low	Not required	None	None	Partial	** DISPUTED ** The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (size.width <= (1<<20)) may be false. Note: "OpenCV CV_Assert is not an assertion (C-like assert()), it is regular C++ exception which can raised in case of invalid or non-supported parameters."
11	CVE-2018-7712	617		DoS	05/03/2018	10/02/2020	5	None	Remote	Low	Not required	None	None	Partial	** DISPUTED ** The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (size.height <= (1<<20)) may be false. Note: "OpenCV CV_Assert is not an assertion (C-like assert()), it is regular C++ exception which can raised in case of invalid or non-supported parameters."
12	CVE-2018-5269	617			08/01/2018	03/10/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	In OpenCV 3.3.1, an assertion failure happens in cv::RBaseStream::setPos in modules/imgcodecs/src/bitstrm.cpp because of an incorrect integer cast.
13	CVE-2018-5268	787		Overflow	08/01/2018	24/08/2020	4,3	None	Remote	Medium	Not required	None	None	Partial	In OpenCV 3.3.1, a heap-based buffer overflow happens in cv::Jpeg2KDecoder::readComponent8u in modules/imgcodecs/src/grfmt_jpeg2000.cpp when parsing a crafted image file.
14	CVE-2017-100045	190		DoS Exec Code Overflow	02/01/2018	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	In opencv/modules/imgcodecs/src/utils.cpp, functions FillUniColor and FillUniGray do not check the input length, which can lead to integer overflow. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.
15	CVE-2017-18009	125			01/01/2018	03/10/2019	5	None	Remote	Low	Not required	None	None	Partial	In OpenCV 3.3.1, a heap-based buffer over-read exists in the function cv::HdrDecoder::checkSignature in modules/imgcodecs/src/grfmt_hdr.cpp.
16	CVE-2017-17760	119		Overflow	29/12/2017	20/03/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	OpenCV 3.3.1 has a Buffer Overflow in the cv::PxMDecoder::readData function in grfmt_pxm.cpp, because an incorrect size value is used.
17	CVE-2017-14136	787			04/09/2017	20/03/2019	4,3	None	Remote	Medium	Not required	None	None	Partial	OpenCV (Open Source Computer Vision Library) 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-12597.
18	CVE-2017-12864	190		DoS Exec Code Overflow	15/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	In opencv/modules/imgcodecs/src/grfmt_pxm.cpp, function ReadNumber did not checkout the input length, which lead to integer overflow. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.
19	CVE-2017-12863	190		DoS Exec Code Overflow	15/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	In opencv/modules/imgcodecs/src/grfmt_pxm.cpp, function PxMDecoder::readData has an integer overflow when calculate src_pitch. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.
20	CVE-2017-12862	119		DoS Exec Code Overflow	15/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	In modules/imgcodecs/src/grfmt_pxm.cpp, the length of buffer AutoBuffer _src is small than expected, which will cause copy buffer overflow later. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.
21	CVE-2017-12606	787			07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the function FillColorRow4 in utils.cpp when reading an image file by using cv::imread.
22	CVE-2017-12605	787			07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the FillColorRow8 function in utils.cpp when reading an image file by using cv::imread.
23	CVE-2017-12604	787			07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the FillUniColor function in utils.cpp when reading an image file by using cv::imread.
24	CVE-2017-12603	787		Overflow	07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an invalid write in the cv::RLByteStream::getBytes function in modules/imgcodecs/src/bitstrm.cpp when reading an image file by using cv::imread, as demonstrated by the 2-opencv-heapoverflow-fseek test case.
25	CVE-2017-12602			DoS	07/08/2017	03/10/2019	7,8	None	Remote	Low	Not required	None	None	Complete	OpenCV (Open Source Computer Vision Library) through 3.3 has a denial of service (memory consumption) issue, as demonstrated by the 10-opencv-dos-memory-exhaust test case.
26	CVE-2017-12601	119		Overflow	07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has a buffer overflow in the cv::BmpDecoder::readData function in modules/imgcodecs/src/grfmt_bmp.cpp when reading an image file by using cv::imread, as demonstrated by the 4-buf-overflow-readData-memcpy test case.
27	CVE-2017-12600			DoS	07/08/2017	03/10/2019	7,8	None	Remote	Low	Not required	None	None	Complete	OpenCV (Open Source Computer Vision Library) through 3.3 has a denial of service (CPU consumption) issue, as demonstrated by the 11-opencv-dos-cpu-exhaust test case.
28	CVE-2017-12599	125			07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds read error in the function icvCvt_BGRA2BGR_8u_C4C3R when reading an image file by using cv::imread.
29	CVE-2017-12598	125			07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds read error in the cv::RBaseStream::readBlock function in modules/imgcodecs/src/bitstrm.cpp when reading an image file by using cv::imread, as demonstrated by the 8-opencv-invalid-read-fread test case.

30	CVE-2017-12597	787			07/08/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread.
31	CVE-2016-1517	20		DoS	10/04/2017	14/04/2017	4,3	None	Remote	Medium	Not required	None	None	Partial	OpenCV 3.0.0 allows remote attackers to cause a denial of service (segfault) via vectors involving corrupt chunks.
32	CVE-2016-1516	415		Exec Code	10/04/2017	20/03/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	OpenCV 3.0.0 has a double free issue that allows attackers to execute arbitrary code.

libcurl

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2012-0036	89		Sql	13/04/2012	10/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	curl and libcurl 7.2x before 7.24.0 do not properly consider special characters during extraction of a pathname from a URL, which allows remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection attack on the (1) IMAP, (2) POP3, or (3) SMTP protocol.
2	CVE-2010-0734	264		DoS	19/03/2010	10/10/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	content_encoding.c in libcurl 7.10.5 through 7.19.7, when zlib is enabled, does not properly restrict the amount of callback data sent to an application that requests automatic decompression, which might allow remote attackers to cause a denial of service (application crash) or have unspecified other impact by sending crafted compressed data to an application that relies on the intended data-length limit.
3	CVE-2009-2417	310			14/08/2009	10/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	lib/ssluse.c in cURL and libcurl 7.4 through 7.19.5, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
4	CVE-2009-0037	352		Exec Code	05/03/2009	11/10/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The redirect implementation in curl and libcurl 5.11 through 7.19.3, when CURLOPT_FOLLOWLOCATION is enabled, accepts arbitrary Location values, which might allow remote HTTP servers to (1) trigger arbitrary requests to intranet servers, (2) read or overwrite arbitrary files via a redirect to a file: URL, or (3) execute arbitrary commands via a redirect to an scp: URL.

libgstreamer

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2016-9813	476		DoS	13/01/2017	05/01/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	The _parse_pat function in the mpegts parser in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.
2	CVE-2016-9812	125		DoS	13/01/2017	05/01/2018	5	None	Remote	Low	Not required	None	None	Partial	The gst_mpegts_section_new function in the mpegts decoder in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a too small section.
3	CVE-2016-9811	125		DoS	13/01/2017	05/01/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	The windows_icon_typefind function in gst-plugins-base in GStreamer before 1.10.2, when G_SLICE is set to always-malloc, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted ico file.
4	CVE-2016-9810	125		DoS	13/01/2017	05/01/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	The gst_decode_chain_free_internal function in the flxdex decoder in gst-plugins-good in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (invalid memory read and crash) via an invalid file, which triggers an incorrect unref call.
5	CVE-2016-9809	125			13/01/2017	05/01/2018	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Off-by-one error in the gst_h264_parse_set_caps function in GStreamer before 1.10.2 allows remote attackers to have unspecified impact via a crafted file, which triggers an out-of-bounds read.
6	CVE-2016-9808	787		DoS	13/01/2017	05/01/2018	5	None	Remote	Low	Not required	None	None	Partial	The FLIC decoder in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (out-of-bounds write and crash) via a crafted series of skip and count pairs.
7	CVE-2016-9807	125		DoS	13/01/2017	05/01/2018	4,3	None	Remote	Medium	Not required	None	None	Partial	The flx_decode_chunks function in gst/flx/gstflxdec.c in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted FLIC file.
8	CVE-2016-9636	119		DoS Exec Code Overflow	27/01/2017	05/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before 1.10.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by providing a 'write count' that goes beyond the initialized buffer.
9	CVE-2016-9635	119		DoS Exec Code Overflow	27/01/2017	05/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before 1.10.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by providing a 'skip count' that goes beyond initialized buffer.
10	CVE-2016-9634	119		DoS Exec Code Overflow	27/01/2017	05/01/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before 1.10.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via the start_line parameter.
11	CVE-2009-1932	189		DoS Exec Code Overflow	04/06/2009	29/09/2017	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Multiple integer overflows in the (1) user_info_callback, (2) user_endrow_callback, and (3) gst_pngdec_task functions (ext/libpng/gstpngdec.c) in GStreamer Good Plug-ins (aka gst-plugins-good or gstreamer-plugins-good) 0.10.15 allow remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted PNG file, which triggers a buffer overflow.
12	CVE-2009-0586	189		Exec Code Overflow	14/03/2009	10/10/2018	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Integer overflow in the gst_vorbis_tag_add_coverart function (gst-libs/gst/tag/gstvorbistag.c) in vorbistag in gst-plugins-base (aka gstreamer-plugins-base) before 0.10.23 in GStreamer allows context-dependent attackers to execute arbitrary code via a crafted COVERART tag that is converted from a base64 representation, which triggers a heap-based buffer overflow.
13	CVE-2009-0398	119		Overflow	03/02/2009	29/09/2017	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	Array index error in the gst_qtp_trak_handler function in gst/qtdemux/qtdemux.c in GStreamer Plug-ins (aka gstreamer-plugins) 0.6.0 allows remote attackers to have an unknown impact via a crafted QuickTime media file.
14	CVE-2009-0397	119		Exec Code Overflow	03/02/2009	11/10/2018	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	Heap-based buffer overflow in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11, and GStreamer Plug-ins (aka gstreamer-plugins) 0.8.5, might allow remote attackers to execute arbitrary code via crafted Time-to-sample (aka stts) atom data in a malformed QuickTime media .mov file.
15	CVE-2009-0387	119		DoS Exec Code Overflow	02/02/2009	11/10/2018	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	Array index error in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted Sync Sample (aka stss) atom data in a malformed QuickTime media .mov file, related to "mark keyframes."
16	CVE-2009-0386	119		Exec Code Overflow	02/02/2009	11/10/2018	9,3	None	Remote	Medium	Not required	Complete	Complete	Complete	Heap-based buffer overflow in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11 might allow remote attackers to execute arbitrary code via crafted Composition Time To Sample (ctts) atom data in a malformed QuickTime media .mov file.

uboot

#	CVE ID	CWE ID	# de Explorações	Tipo(s) de vulnerabilidades	Data de publicação	Data de atualização	Pontuação	Nível de Acesso Ganho	Acesse	Complexidade	Autenticação	Configuração	Integração	Disponibilidade	
1	CVE-2021-27138				17/02/2021	24/02/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The boot loader in Das U-Boot before 2021.04-rc2 mishandles use of unit addresses in a FIT.
2	CVE-2021-27097				17/02/2021	23/02/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	The boot loader in Das U-Boot before 2021.04-rc2 mishandles a modified FIT.
3	CVE-2020-10648	20		Bypass	19/03/2020	26/03/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Das U-Boot through 2020.01 allows attackers to bypass verified boot restrictions and subsequently boot arbitrary images by providing a crafted FIT image to a system configured to boot the default configuration.
4	CVE-2020-8432	415		Exec Code	29/01/2020	21/07/2021	10	None	Remote	Low	Not required	Complete	Complete	Complete	In Das U-Boot through 2020.01, a double free has been found in the cmd/gpt.c do_rename_gpt_parts() function. Double freeing may result in a write-what-where condition, allowing an attacker to execute arbitrary code. NOTE: this vulnerablity was introduced when attempting to fix a memory leak identified by static analysis.
5	CVE-2019-14204	787		Overflow	31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_umountall_reply.
6	CVE-2019-14203	787		Overflow	31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_mount_reply.
7	CVE-2019-14202	787		Overflow	31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_readlink_reply.
8	CVE-2019-14201	787		Overflow	31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_lookup_reply.
9	CVE-2019-14200	787		Overflow	31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: rpc_lookup_reply.
10	CVE-2019-14199	191			31/07/2019	02/08/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an *udp_packet_handler call.
11	CVE-2019-14198	787			31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv3 case.
12	CVE-2019-14197	125			31/07/2019	02/08/2019	6,4	None	Remote	Low	Not required	Partial	None	Partial	An issue was discovered in Das U-Boot through 2019.07. There is a read of out-of-bounds data at nfs_read_reply.
13	CVE-2019-14196	787			31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_lookup_reply.
14	CVE-2019-14195	787			31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with unvalidated length at nfs_readlink_reply in the "else" block after calculating the new path length.
15	CVE-2019-14194	787			31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv2 case.
16	CVE-2019-14193	787			31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with an unvalidated length at nfs_readlink_reply, in the "if" block after calculating the new path length.
17	CVE-2019-14192	787			31/07/2019	24/08/2020	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an nc_input_packet call.
18	CVE-2019-13106	787		Exec Code Overflow	06/08/2019	01/10/2019	8,3	None	Remote	Medium	Not required	Partial	Partial	Complete	Das U-Boot versions 2016.09 through 2019.07-rc4 can memset() too much data while reading a crafted ext4 filesystem, which results in a stack buffer overflow and likely code execution.
19	CVE-2019-13105	415			06/08/2019	13/08/2019	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	Das U-Boot versions 2019.07-rc1 through 2019.07-rc4 can double-free a cached block of data when listing files in a crafted ext4 filesystem.
20	CVE-2019-13104	119		Overflow	06/08/2019	21/07/2021	6,8	None	Remote	Medium	Not required	Partial	Partial	Partial	In Das U-Boot versions 2016.11-rc1 through 2019.07-rc4, an underflow can cause memcpy() to overwrite a very large amount of data (including the whole stack) while reading a crafted ext4 filesystem.
21	CVE-2019-13103	674			29/07/2019	24/08/2020	3,6	None	Local	Low	Not required	None	Partial	Partial	A crafted self-referential DOS partition table will cause all Das U-Boot versions through 2019.07-rc4 to infinitely recurse, causing the stack to grow infinitely and eventually either crash or overwrite other data.
22	CVE-2019-11690	330			03/05/2019	06/05/2019	4,3	None	Remote	Medium	Not required	Partial	None	None	gen_rand_uuid in lib/uuid.c in Das U-Boot v2014.04 through v2019.04 lacks an srand call, which allows attackers to determine UUID values in scenarios where CONFIG_RANDOM_UUID is enabled, and Das U-Boot is relied upon for UUID values of a GUID Partition Table of a boot device.
23	CVE-2019-11059	119		Overflow	10/05/2019	13/05/2019	7,5	None	Remote	Low	Not required	Partial	Partial	Partial	Das U-Boot 2016.11-rc1 through 2019.04 mishandles the ext4 64-bit extension, resulting in a buffer overflow.
24	CVE-2018-100020	20		Bypass	26/06/2018	22/10/2020	4,3	None	Remote	Medium	Not required	None	Partial	None	U-Boot contains a CWE-20: Improper Input Validation vulnerability in Verified boot signature validation that can result in Bypass verified boot. This attack appear to be exploitable via Specially crafted FIT image and special device memory functionality.
25	CVE-2018-18440	119		Overflow	20/11/2018	10/12/2019	7,2	None	Local	Low	Not required	Complete	Complete	Complete	DENX U-Boot through 2018.09-rc1 has a locally exploitable buffer overflow via a crafted kernel image because filesystem loading is mishandled.
26	CVE-2018-3968	347		Bypass	21/03/2019	02/04/2019	4,4	None	Local	Medium	Not required	Partial	Partial	Partial	An exploitable vulnerability exists in the verified boot protection of the Das U-Boot from version 2013.07-rc1 to 2014.07-rc2. The affected versions lack proper FIT signature enforcement, which allows an attacker to bypass U-Boot's verified boot and execute an unsigned kernel, embedded in a legacy image format. To trigger this vulnerability, a local attacker needs to be able to supply the image to boot.
27	CVE-2017-3226	310			24/07/2018	09/10/2019	4,4	None	Local	Medium	Not required	Partial	Partial	Partial	Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. Devices that make use of Das U-Boot's AES-CBC encryption feature using environment encryption (i.e., setting the configuration parameter CONFIG_ENV_AES=y) read environment variables from disk as the encrypted disk image is processed. An attacker with physical access to the device can manipulate the encrypted environment data to include a crafted two-byte sequence which triggers an errc
28	CVE-2017-3225	310			24/07/2018	09/10/2019	2,1	None	Local	Low	Not required	Partial	None	None	Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. For devices utilizing this environment encryption mode, U-Boot's use of a zero initialization vector may allow attacks against the underlying cryptographic implementation and allow an attacker to decrypt the data. Das U-Boot's AES-CBC encryption feature uses a zero (0) initialization vector. This allows an attacker to perform dictionary attacks on encrypted data produced by Das U-Boot to learn inform

ns. In other words, the reference to 2.23 is intentional despite the mention of "Fixed for glibc 2.33" in the 26649 reference.

his memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.

ed program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.

en it is inappropriate within a specific environment.

ns, 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.

so it is not a vulnerability.

08-4113.

t.

standard (aka ISO/IEC 9899:1999).

ns. In other words, the reference to 2.23 is intentional despite the mention of "Fixed for glibc 2.33" in the 26649 reference.

his memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.

ed program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.

ent vulnerability than CVE-2012-3404 and CVE-2012-3405.

cted that any standard operating-system distribution would ship an applicable setuid or setgid program.

RCE) implementations.

ıme character, related to a "decompression bomb" attack.

r in environment variable parsing. This error condition is improperly handled by Das U-Boot, resulting in an immediate process termination with a debugging message.
ation about the encrypted data.