CVE Details
The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View C\

Log In Register
Vulnerability Feeds & Widgets New www.itsecdb.com

Security Vulnerabilities Published In 2018(Overflow)

2018 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2018-1999011</td><td>119</td><td></td><td>Exec Code Overflow</td><td>2018-07-23</td><td>2019-05-23</td><td>6.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">FFmpeg before commit 2b46ebdbff1d8dec7a3d8ea280a612b91a582869 contains a Buffer Overflow vulnerability in asf_o format demuxer that can result in heap-buffer-overflow that may result in remote code execution. This attack appears to be exploitable via specially crafted ASF file that has to be provided as input to FFmpeg. This vulnerability appears to have been fixed in 2b46ebdbff1d8dec7a3d8ea280a612b91a582869 and later.</td></tr>
<tr><td>2</td><td>CVE-2018-1000886</td><td></td><td></td><td>Overflow</td><td>2018-12-20</td><td>2018-12-20</td><td>0.0</td><td>None</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td></tr>
<tr><td colspan="15">nasm version 2.14.01rc5, 2.15 contains a Buffer Overflow vulnerability in asm/stdscan.c:130 that can result in Stack-overflow caused by triggering endless macro generation, crash the program. This attack appear to be exploitable via a crafted nasm input file.</td></tr>
<tr><td>3</td><td>CVE-2018-1000876</td><td>190</td><td></td><td>Exec Code Overflow</td><td>2018-12-20</td><td>2019-08-06</td><td>4.6</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.</td></tr>
<tr><td>4</td><td>CVE-2018-1000810</td><td>190</td><td></td><td>Overflow</td><td>2018-10-08</td><td>2019-01-04</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">The Rust Programming Language Standard Library version 1.29.0, 1.28.0, 1.27.2, 1.27.1, 127.0, 126.2, 126.1, 126.0 contains a CWE-680: Integer Overflow to Buffer Overflow vulnerability in standard library that can result in buffer overflow. This attack appear to be exploitable via str::repeat, passed a large number, can overflow an internal buffer. This vulnerability appears to have been fixed in 1.29.1.</td></tr>
<tr><td>5</td><td>CVE-2018-1000804</td><td>119</td><td></td><td>Exec Code Overflow Sql</td><td>2018-10-08</td><td>2019-09-27</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">contiki-ng version 4 contains a Buffer Overflow vulnerability in AQL (Antelope Query Language) database engine that can result in Attacker can perform Remote Code Execution on device using Contiki-NG operating system. This attack appear to be exploitable via Attacker must be able to run malicious AQL code (e.g. via SQL-like Injection attack).</td></tr>
<tr><td>6</td><td>CVE-2018-1000667</td><td>119</td><td></td><td>Overflow Mem. Corr.</td><td>2018-09-06</td><td>2018-11-01</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">NASM nasm-2.13.03 nasm- 2.14rc15 version 2.14rc15 and earlier contains a memory corruption (crashed) of nasm when handling a crafted file due to function assemble_file(inname, depend_ptr) at asm/nasm.c:482. vulnerability in function assemble_file(inname, depend_ptr) at asm/nasm.c:482. that can result in aborting/crash nasm program. This attack appear to be exploitable via a specially crafted asm file..</td></tr>
<tr><td>7</td><td>CVE-2018-1000663</td><td>119</td><td></td><td>Exec Code Overflow</td><td>2018-09-06</td><td>2018-10-25</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">jsish version 2.4.70 2.047 contains a Buffer Overflow vulnerability in function _jsi_evalcode from jsiEval.c that can result in Crash due to segmentation fault. This attack appear to be exploitable via The victim must execute crafted javascript code.</td></tr>
<tr><td>8</td><td>CVE-2018-1000657</td><td>119</td><td></td><td>Exec Code Overflow</td><td>2018-08-20</td><td>2018-10-18</td><td>4.6</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">Rust Programming Language Rust standard library version Commit bfa0e1f58acf1c28d500c34ed258f09ae021893e and later; stable release 1.3.0 and later contains a Buffer Overflow vulnerability in std::collections::vec_deque::VecDeque::reserve() function that can result in Arbitrary code execution, but no proof-of-concept exploit is currently published.. This vulnerability appears to have been fixed in after commit fdfafb510b1a38f727e920dccbeeb638d39a8e60; stable release 1.22.0 and later.</td></tr>
<tr><td>9</td><td>CVE-2018-1000637</td><td>119</td><td></td><td>DoS Exec Code Overflow</td><td>2018-08-20</td><td>2018-11-02</td><td>6.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">zutils version prior to version 1.8-pre2 contains a Buffer Overflow vulnerability in zcat that can result in Potential denial of service or arbitrary code execution. This attack appear to be exploitable via the victim openning a crafted compressed file. This vulnerability appears to have been fixed in 1.8-pre2.</td></tr>
<tr><td>10</td><td>CVE-2018-1000618</td><td>119</td><td></td><td>Overflow</td><td>2018-07-09</td><td>2018-09-12</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">EOSIO/eos eos version after commit f1545dd0ae2b77580c2236fdb70ae7138d2c7168 contains a stack overflow vulnerability in abi_serializer that can result in attack eos network node. This attack appear to be exploitable via network request. This vulnerability appears to have been fixed in after commit cf7209e703e6d3f7a5413e0cb1fe88a4d8e4b38d .</td></tr>
<tr><td>11</td><td>CVE-2018-1000537</td><td>119</td><td></td><td>Exec Code Overflow</td><td>2018-06-26</td><td>2018-08-31</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">Marlin Firmware Marlin version 1.1.x and earlier contains a Buffer Overflow vulnerability in cardreader.cpp (Depending on branch/version) that can result in Arbitrary code execution. This attack appear to be exploitable via Crafted G-Code instruction/file is sent to the printer.</td></tr>
<tr><td>12</td><td>CVE-2018-1000524</td><td>190</td><td></td><td>DoS Overflow</td><td>2018-06-26</td><td>2018-08-28</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">miniSphere version 5.2.9 and earlier contains a Integer Overflow vulnerability in layer_resize() function in map_engine.c that can result in remote denial of service. This attack appear to be exploitable via the victim must load a specially-crafted map which calls SetLayerSize in its entry script. This vulnerability appears to have been fixed in 5.0.3, 5.1.5, 5.2.10 and later.</td></tr>
<tr><td>13</td><td>CVE-2018-1000517</td><td>119</td><td></td><td>Overflow</td><td>2018-06-26</td><td>2019-04-03</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">BusyBox project BusyBox wget version prior to commit 8e2174e9bd836e53c8b9c6e00d1bc6e2a718686e contains a Buffer Overflow vulnerability in Busybox wget that can result in heap buffer overflow. This attack appear to be exploitable via network connectivity. This vulnerability appears to have been fixed in after commit 8e2174e9bd836e53c8b9c6e00d1bc6e2a718686e.</td></tr>
<tr><td>14</td><td>CVE-2018-1000300</td><td>119</td><td></td><td>DoS Overflow</td><td>2018-05-24</td><td>2019-03-29</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">curl version curl 7.54.1 to and including curl 7.59.0 contains a CWE-122: Heap-based Buffer Overflow vulnerability in denial of service and more that can result in curl might overflow a heap based memory buffer when closing down an FTP connection with very long server command replies.. This vulnerability appears to have been fixed in curl < 7.54.1 and curl >= 7.60.0.</td></tr>
<tr><td>15</td><td>CVE-2018-1000224</td><td>502</td><td></td><td>Overflow</td><td>2018-08-20</td><td>2018-10-31</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
</table>

Home
Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :
- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :
- NVD Website
- CWE Web Site

View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :
Go
(e.g.: 12345)

Search By Microsoft Reference ID:
Go
(e.g.: ms10-001 or 979352)

Godot Engine version All versions prior to 2.1.5, all 3.0 versions prior to 3.0.6. contains a Signed/unsigned comparison, wrong buffer size chackes, integer overflow, missing padding initialization vulnerability in (De)Serialization functions (core/io/marshalls.cpp) that can result in DoS (packet of death), possible leak of uninitialized memory. This attack appear to be exploitable via A malformed packet is received over the network by a Godot application that uses built-in serialization (e.g. game server, or game client). Could be triggered by multiplayer opponent. This vulnerability appears to have been fixed in 2.1.5, 3.0.6, master branch after commit feaf03421dda0213382b51aff07bd5a96b29487b.													
16	CVE-2018-1000223	119	Exec Code Overflow	2018-08-20	2018-10-15	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
soundtouch version up to and including 2.0.0 contains a Buffer Overflow vulnerability in SoundStretch/WavFile.cpp:WavInFile::readHeaderBlock() that can result in arbitrary code execution. This attack appear to be exploitable via victim must open maliocius file in soundstretch utility.													
17	CVE-2018-1000221	119	Overflow	2018-08-20	2018-10-15	**7.5**	None	Remote	Low	Not required	Partial	Partial	Partial
pkgconf version 1.5.0 to 1.5.2 contains a Buffer Overflow vulnerability in dequote() that can result in dequote() function returns 1-byte allocation if initial length is 0, leading to buffer overflow. This attack appear to be exploitable via specially crafted .pc file. This vulnerability appears to have been fixed in 1.5.3.													
18	CVE-2018-1000178	119	Exec Code Overflow	2018-05-08	2018-10-21	**7.5**	None	Remote	Low	Not required	Partial	Partial	Partial
A heap corruption of type CWE-120 exists in quassel version 0.12.4 in quasselcore in void DataStreamPeer::processMessage(const QByteArray &msg) datastreampeer.cpp line 62 that allows an attacker to execute code remotely.													
19	CVE-2018-1000140	119	Exec Code Overflow	2018-03-23	2019-05-01	**7.5**	None	Remote	Low	Not required	Partial	Partial	Partial
rsyslog librelp version 1.2.14 and earlier contains a Buffer Overflow vulnerability in the checking of x509 certificates from a peer that can result in Remote code execution. This attack appear to be exploitable a remote attacker that can connect to rsyslog and trigger a stack buffer overflow by sending a specially crafted x509 certificate.													
20	CVE-2018-1000128		Exec Code Overflow	2018-03-13	2018-03-13	**0.0**	None	???	???	???	???	???	???
GPAC MP4Box version prior to commit 90dc7f853d31b0a4e9441cba97feccf36d8b69a4 contains a Buffer Overflow vulnerability in src/media_tools/av_parsers.c, lines 2387-2388: https://github.com/gpac/gpac/blob/84c4e606a1f906cd4b07ad94d19cea2b668f64ad/src/media_tools/av_parsers.c#L2387-L2388 that can result in may allow an attacker to achieve remote code execution. This attack appear to be exploitable via The victim must open a specially crafted MP4 file. This vulnerability appears to have been fixed in after commit 90dc7f853d31b0a4e9441cba97feccf36d8b69a4.													
21	CVE-2018-1000127	190	Overflow	2018-03-13	2019-09-06	**5.0**	None	Remote	Low	Not required	None	None	Partial
memcached version prior to 1.4.37 contains an Integer Overflow vulnerability in items.c:item_free() that can result in data corruption and deadlocks due to items existing in hash table being reused from free list. This attack appear to be exploitable via network connectivity to the memcached service. This vulnerability appears to have been fixed in 1.4.37 and later.													
22	CVE-2018-1000120	787	DoS Overflow	2018-03-14	2019-06-18	**7.5**	None	Remote	Low	Not required	Partial	Partial	Partial
A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.													
23	CVE-2018-1000117	119	Exec Code Overflow	2018-03-07	2018-03-29	**7.2**	None	Local	Low	Not required	Complete	Complete	Complete
Python Software Foundation CPython version From 3.2 until 3.6.4 on Windows contains a Buffer Overflow vulnerability in os.symlink() function on Windows that can result in Arbitrary code execution, likely escalation of privilege. This attack appears to be exploitable via a python script that creates a symlink with an attacker controlled name or location. This vulnerability appears to have been fixed in 3.7.0 and 3.6.5.													
24	CVE-2018-1000116	119	Exec Code Overflow	2018-03-07	2018-03-29	**7.5**	None	Remote	Low	Not required	Partial	Partial	Partial
NET-SNMP version 5.7.2 contains a heap corruption vulnerability in the UDP protocol handler that can result in command execution.													
25	CVE-2018-1000101	119	Overflow	2018-03-06	2018-03-29	**7.5**	None	Remote	Low	Not required	Partial	Partial	Partial
Mingw-w64 version 5.0.3 and earlier contains an Improper Null Termination (CWE-170) vulnerability in mingw-w64-crt (libc)->(v)snprintf that can result in The bug may be used to corrupt subsequent string functions. This attack appear to be exploitable via Depending on the usage, worst case: network.													
26	CVE-2018-1000100	119	Overflow	2018-03-06	2019-04-03	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
GPAC MP4Box version 0.7.1 and earlier contains a Buffer Overflow vulnerability in src/isomedia/avc_ext.c lines 2417 to 2420 that can result in Heap chunks being modified, this could lead to RCE. This attack appear to be exploitable via an attacker supplied MP4 file that when run by the victim may result in RCE.													
27	CVE-2018-1000098	190	Overflow	2018-03-12	2018-04-11	**5.0**	None	Remote	Low	Not required	None	None	Partial
Teluu PJSIP version 2.7.1 and earlier contains a Integer Overflow vulnerability in pjmedia SDP parsing that can result in Crash. This attack appear to be exploitable via Sending a specially crafted message. This vulnerability appears to have been fixed in 2.7.2.													
28	CVE-2018-1000097	119	Exec Code Overflow	2018-03-12	2018-04-13	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
Sharutils sharutils (unshar command) version 4.15.2 contains a Buffer Overflow vulnerability in Affected component on the file unshar.c at line 75, function looks_like_c_code. Failure to perform checking of the buffer containing input line. that can result in Could lead to code execution. This attack appear to be exploitable via Victim have to run unshar command on a specially crafted file..													
29	CVE-2018-1000091	119	Exec Code Overflow	2018-03-13	2018-04-10	**6.5**	None	Remote	Low	Single system	Partial	Partial	Partial
KadNode version version 2.2.0 contains a Buffer Overflow vulnerability in Arguments when starting up the binary that can result in Control of program execution flow, leading to remote code execution.													
30	CVE-2018-1000052	119	DoS Overflow Mem. Corr.	2018-02-09	2018-03-08	**5.0**	None	Remote	Low	Not required	None	None	Partial
fmtlib version prior to version 4.1.0 (before commit 0555cea5fc0bf890afe0071a558e44625a34ba85) contains a Memory corruption (SIGSEGV), CWE-134 vulnerability in fmt::print() library function that can result in Denial of Service. This attack appear to be exploitable via Specifying an invalid format specifier in the fmt::print() function results in a SIGSEGV (memory corruption, invalid write). This vulnerability appears to have been fixed in after commit 8cf30aa2be256eba07bb1cefb998c52326e846e7.													
31	CVE-2018-1000050	119	DoS Overflow Mem. Corr.	2018-02-09	2018-03-08	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
Sean Barrett stb_vorbis version 1.12 and earlier contains a Buffer Overflow vulnerability in All vorbis decoding paths. that can result in memory corruption, denial of service, comprised execution of host program. This attack appear to be exploitable via Victim must open a specially crafted Ogg Vorbis file. This vulnerability appears to have been fixed in 1.13.													
32	CVE-2018-1000038	119	Exec Code Overflow	2018-05-24	2018-11-27	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
In MuPDF 1.12.0 and earlier, a stack buffer overflow in function pdf_lookup_cmap_full in pdf/pdf-cmap.c could allow an attacker to execute arbitrary code via a crafted file.													
33	CVE-2018-1000035	119	DoS Exec Code Overflow	2018-02-09	2018-02-26	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
A heap-based buffer overflow exists in Info-Zip UnZip version <= 6.00 in the processing of password-protected archives that allows an attacker to perform a denial of service or to possibly achieve code execution.													

34	CVE-2018-1000032	119	DoS Exec Code Overflow	2018-02-09	2018-02-26	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
A heap-based buffer overflow exists in Info-Zip UnZip version 6.10c22 that allows an attacker to perform a denial of service or to possibly achieve code execution.													
35	CVE-2018-1000031	119	DoS Exec Code Overflow	2018-02-09	2018-02-26	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
A heap-based buffer overflow exists in Info-Zip UnZip version 6.10c22 that allows an attacker to perform a denial of service or to possibly achieve code execution.													
36	CVE-2018-1000030	119	Overflow Mem. Corr.	2018-02-08	2019-10-09	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.													
37	CVE-2018-20617	119	Overflow	2018-12-31	2019-01-10	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_csv_decode2 function in ok_csv.c.													
38	CVE-2018-20616	119	Overflow	2018-12-31	2019-01-10	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_wav_decode_ms_adpcm_data function in ok_wav.c.													
39	CVE-2018-20593	119	Overflow	2018-12-30	2019-04-03	**4.3**	None	Remote	Medium	Not required	None	None	Partial
In Mini-XML (aka mxml) v2.12, there is stack-based buffer overflow in the scan_file function in mxmldoc.c.													
40	CVE-2018-20584	119	DoS Overflow	2018-12-30	2019-08-09	**4.3**	None	Remote	Medium	Not required	None	None	Partial
JasPer 2.0.14 allows remote attackers to cause a denial of service (application hang) via an attempted conversion to the jp2 format.													
41	CVE-2018-20579	119	Overflow	2018-12-28	2019-01-14	**3.6**	None	Local	Low	Not required	None	Partial	Partial
Contiki-NG before 4.2 has a stack-based buffer overflow in the push function in os/lib/json/jsonparse.c that allows an out-of-bounds write of an '{' or '[' character.													
42	CVE-2018-20574	119	DoS Overflow	2018-12-28	2019-01-10	**4.3**	None	Remote	Medium	Not required	None	None	Partial
The SingleDocParser::HandleFlowMap function in yaml-cpp (aka LibYaml-C++) 0.6.2 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted YAML file.													
43	CVE-2018-20573	119	DoS Overflow	2018-12-28	2019-01-10	**4.3**	None	Remote	Medium	Not required	None	None	Partial
The Scanner::EnsureTokensInQueue function in yaml-cpp (aka LibYaml-C++) 0.6.2 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted YAML file.													
44	CVE-2018-20542	119	Overflow	2018-12-28	2019-01-11	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
There is a heap-based buffer-overflow at generator_spgemm_csc_reader.c (function libxsmm_sparse_csc_reader) in LIBXSMM 1.10, a different vulnerability than CVE-2018-20541 (which is in a different part of the source code and is seen at a different address).													
45	CVE-2018-20541	119	Overflow	2018-12-28	2019-01-11	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
There is a heap-based buffer overflow in libxsmm_sparse_csc_reader at generator_spgemm_csc_reader.c in LIBXSMM 1.10, a different vulnerability than CVE-2018-20542 (which is in a different part of the source code and is seen at different addresses).													
46	CVE-2018-20534	119	DoS Overflow	2018-12-28	2019-10-02	**4.3**	None	Remote	Medium	Not required	None	None	Partial
** DISPUTED ** There is an illegal address access at ext/testcase.c in libsolv.a in libsolv through 0.7.2 that will cause a denial of service. NOTE: third parties dispute this issue stating that the issue affects the test suite and not the underlying library. It cannot be exploited in any real-world application.													
47	CVE-2018-20460	119	Overflow	2018-12-25	2018-12-31	**4.3**	None	Remote	Medium	Not required	None	None	Partial
In radare2 prior to 3.1.2, the parseOperands function in libr/asm/arch/arm/armass64.c allows attackers to cause a denial-of-service (application crash caused by stack-based buffer overflow) by crafting an input file.													
48	CVE-2018-20455	119	DoS Overflow	2018-12-25	2018-12-31	**4.3**	None	Remote	Medium	Not required	None	None	Partial
In radare2 prior to 3.1.1, the parseOperand function inside libr/asm/p/asm_x86_nz.c may allow attackers to cause a denial of service (application crash via a stack-based buffer overflow) by crafting an input file, a related issue to CVE-2018-20456.													
49	CVE-2018-20452	119	DoS Overflow	2018-12-25	2019-01-11	**6.8**	None	Remote	Medium	Not required	Partial	Partial	Partial
The read_MSAT_body function in ole.c in libxls 1.4.0 has an invalid free that allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, because of inconsistent memory management (new versus free) in ole2_read_header in ole.c.													
50	CVE-2018-20410		Overflow	2018-12-23	2018-12-23	**0.0**	None	???	???	???	???	???	???
WellinTech KingSCADA before 3.7.0.0.1 contains a stack-based buffer overflow. The vulnerability is triggered when sending a specially crafted packet to the AlarmServer (AEserver.exe) service listening on TCP port 12401.													

Total number of vulnerabilities : **2368** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback