root add pdf2xml poc readme ... on Jul 5, 2020 History

..	
00-NULL-pointer-dereference-TextPage-restoreState.pdf	2 years ago
01-Heap-buffer-overflow-TextPage-dump.pdf	2 years ago
02-Heap-buffer-overflow-addAttributsNode.pdf	2 years ago
03-Unknow-pointer-dereference-TextPage-restoreState.pdf	2 years ago
04-Memory leaks-TextPage-testLinkedText.pdf	2 years ago
05-Stack-buffer-overflow-XRef-getObjectStream.pdf	2 years ago
readme.md	2 years ago

readme.md

00-NULL-pointer-dereference-TextPage-restoreState.pdf

```
$ gdb ./pdf2xml
(gdb) r 00-NULL-pointer-dereference-TextPage-restoreState.pdf test.xml

Program received signal SIGSEGV, Segmentation fault.
0x000000000040e29b in TextPage::restoreState (state=0x7a02a0, this=0x7a2100) at /home/test/pdf2xml/src/XmlOutputDev.cc:2765
2765            idCur = idStack.top();
(gdb) bt
#0  0x000000000040e29b in TextPage::restoreState (state=0x7a02a0, this=0x7a2100) at /home/test/pdf2xml/src/XmlOutputDev.cc:2765
#1  XmlOutputDev::restoreState (this=<optimized out>, state=0x7a02a0) at /home/test/pdf2xml/src/XmlOutputDev.cc:4333
#2  0x0000000000049983b in Gfx::execOp (this=this@entry=0x7a0140, cmd=cmd@entry=0x7fffffffdf20, args=args@entry=0x7fffffffdf30,
numArgs=numArgs@entry=0) at /home/test/pdf2xml/xpdf/xpdf/Gfx.cc:834
#3  0x0000000000499a4f in Gfx::go (this=this@entry=0x7a0140, topLevel=topLevel@entry=1) at /home/test/pdf2xml/xpdf/xpdf/Gfx.cc:709
#4  0x0000000000499e66 in Gfx::display (this=this@entry=0x7a0140, objRef=objRef@entry=0x7a0120, topLevel=topLevel@entry=1) at
/home/test/pdf2xml/xpdf/xpdf/Gfx.cc:642
#5  0x0000000000465f23 in Page::displaySlice (this=0x7a00f0, out=0x79eae0, out@entry=0x0, hDPI=72, hDPI@entry=0, vDPI=72,
vDPI@entry=3.9364818670782154e-317, rotate=<optimized out>,
    rotate@entry=4612527, useMediaBox=useMediaBox@entry=1, crop=crop@entry=1, sliceX=sliceX@entry=-1, sliceY=-1, sliceW=-1,
sliceH=-1, printing=0, abortCheckCbk=0x0, abortCheckCbkData=0x0)
    at /home/test/pdf2xml/xpdf/xpdf/Page.cc:360
#6  0x00000000004661af in Page::display (this=<optimized out>, out=out@entry=0x0, hDPI=hDPI@entry=0,
vDPI=vDPI@entry=3.9364818670782154e-317, rotate=rotate@entry=4612527,
    useMediaBox=useMediaBox@entry=1, crop=crop@entry=1, printing=printing@entry=0, abortCheckCbk=0x0, abortCheckCbkData=0x0) at
/home/test/pdf2xml/xpdf/xpdf/Page.cc:310
#7  0x00000000004466ffb in PDFDoc::displayPage (this=this@entry=0x799328, out=0x0, out@entry=0x79eae0, page=page@entry=1, hDPI=0,
hDPI@entry=72, vDPI=3.9364818670782154e-317, vDPI@entry=72,
    rotate=4612527, rotate@entry=0, useMediaBox=useMediaBox@entry=1, crop=crop@entry=1, printing=0, abortCheckCbk=0x0,
abortCheckCbkData=0x0) at /home/test/pdf2xml/xpdf/xpdf/PDFDoc.cc:386
#8  0x0000000000046707e in PDFDoc::displayPages (this=this@entry=0x799328, out=out@entry=0x79eae0, firstPage=firstPage@entry=1,
lastPage=lastPage@entry=1, hDPI=hDPI@entry=72, vDPI=vDPI@entry=72,
    rotate=rotate@entry=0, useMediaBox=useMediaBox@entry=1, crop=1, printing=0, abortCheckCbk=0x0, abortCheckCbkData=0x0) at
/home/test/pdf2xml/xpdf/xpdf/PDFDoc.cc:398
#9  0x000000000040d36b in PDFDocXrce::displayPages (this=this@entry=0x799320, out=out@entry=0x79eae0, docrootA=docrootA@entry=0x0,
firstPage=1, lastPage=1, hDPI=hDPI@entry=72, vDPI=vDPI@entry=72,
    rotate=rotate@entry=0, useMediaBox=1, crop=1, doLinks=0, abortCheckCbk=0x0, abortCheckCbkData=0x0) at
/home/test/pdf2xml/src/PDFDocXrce.cc:34
#10 0x0000000000405589 in main (argc=2, argv=<optimized out>) at /home/test/pdf2xml/src/pdftoxml.cc:409
(gdb) x/10i $rip
=> 0x40e29b <XmlOutputDev::restoreState(GfxState*)+171>:        mov    0x1fc(%rcx),%esi
   0x40e2a1 <XmlOutputDev::restoreState(GfxState*)+177>:        mov    %esi,0x180(%rbx)
   0x40e2a7 <XmlOutputDev::restoreState(GfxState*)+183>:        callq  0x402fa0 <_ZdlPv@plt>
   0x40e2ac <XmlOutputDev::restoreState(GfxState*)+188>:        mov    0x178(%rbx),%rdi
   0x40e2b3 <XmlOutputDev::restoreState(GfxState*)+195>:        lea    -0x8(%rdi),%r8
   0x40e2b7 <XmlOutputDev::restoreState(GfxState*)+199>:        mov    %r8,0x178(%rbx)
   0x40e2be <XmlOutputDev::restoreState(GfxState*)+206>:        mov    -0x8(%rdi),%r9
   0x40e2c2 <XmlOutputDev::restoreState(GfxState*)+210>:        lea    0x200(%r9),%r10
   0x40e2c9 <XmlOutputDev::restoreState(GfxState*)+217>:        mov    %r9,0x168(%rbx)
   0x40e2d0 <XmlOutputDev::restoreState(GfxState*)+224>:        add    $0x1fc,%r9
(gdb) p/x $rcx
$1 = 0x0

Function : TextPage::restoreState
Type: null-pointer
```

01-Heap-buffer-overflow-TextPage-dump.pdf

```
$ ./pdf2xml 01-Heap-buffer-overflow-TextPage-dump.pdf test.xml

=================================================================
==36659==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200004405a at pc 0x7fb7e473d9f5 bp 0x7ffc8a9d8c60 sp
0x7ffc8a9d83f0
```

```
WRITE of size 11 at 0x60200004405a thread T0
    #0 0x7fb7e473d9f4 in __interceptor_vsprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x619f4)
    #1 0x7fb7e473dcc9 in __interceptor_sprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x61cc9)
    #2 0x419e84 in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:2001
    #3 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
    #4 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
    #5 0x45633a in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:394
    #6 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310
    #7 0x45740d in PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/PDFDoc.cc:398
    #8 0x407de8 in PDFDocXrce::displayPages(OutputDev*, _xmlNode*, int, int, double, double, int, int, int, int, int (*)(void*),
void*) /home/test/pdf2xml_analysis/pdf2xml/src/PDFDocXrce.cc:34
    #9 0x40943b in main /home/test/pdf2xml_analysis/pdf2xml/src/pdftoxml.cc:409
    #10 0x7fb7e321182f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #11 0x403d28 in _start (/home/test/pdf2xml_analysis/pdf2xml/pdf2xml+0x403d28)

0x60200004405a is located 0 bytes to the right of 10-byte region [0x602000044050,0x60200004405a)
allocated by thread T0 here:
    #0 0x7fb7e4774602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x416b22 in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1652
    #2 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
    #3 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
    #4 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __interceptor_vsprintf
Shadow bytes around the buggy address:
  0x0c04800007b0: fa fa 00 fa fa fa 00 02 fa fa 00 fa fa fa 00 00
  0x0c04800007c0: fa fa 00 fa fa fa fd fa fa fa 00 fa fa fa 00 00
  0x0c04800007d0: fa fa fd fa fa fa fd fd fa fa 06 fa fa fa 03 fa
  0x0c04800007e0: fa fa fd fd fa fa fd fa fa fa fd fd fa fa 06 fa
  0x0c04800007f0: fa fa 04 fa fa fa fd fd fa fa fd fa fa fa fd fd
=>0x0c0480000800: fa fa 06 fa fa fa 05 fa fa fa 00[02]fa fa 00 fa
  0x0c0480000810: fa fa fd fa fa fa 00 fa fa fa fd fa fa fa fd fa
  0x0c0480000820: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 05 fa
  0x0c0480000830: fa fa 07 fa fa fa 00 fa fa fa 02 fa fa fa 00 fa
  0x0c0480000840: fa fa 02 fa fa fa 02 fa fa fa 00 fa fa fa 02 fa
  0x0c0480000850: fa fa 00 fa fa fa 02 fa fa fa 02 fa fa fa 00 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==36659==ABORTING

Function : TextPage::dump
Type: heap-overflow
```

02-Heap-buffer-overflow-addAttributsNode.pdf

```
$ ./pdf2xml 02-Heap-buffer-overflow-addAttributsNode.pdf test.xml

=================================================================
==57105==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200004999a at pc 0x7f0869e219f5 bp 0x7fffaa6b3610 sp
0x7fffaa6b2da0
WRITE of size 12 at 0x60200004999a thread T0
    #0 0x7f0869e219f4 in __interceptor_vsprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x619f4)
    #1 0x7f0869e21cc9 in __interceptor_sprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x61cc9)
    #2 0x414e3d in TextPage::addAttributsNode(_xmlNode*, TextWord*, double&, double&, double&, double&, double&, double&)
/home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1423
    #3 0x417c7c in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1815
    #4 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
    #5 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
    #6 0x45633a in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:394
    #7 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310
    #8 0x45740d in PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/PDFDoc.cc:398
    #9 0x407de8 in PDFDocXrce::displayPages(OutputDev*, _xmlNode*, int, int, double, double, int, int, int, int, int (*)(void*),
void*) /home/test/pdf2xml_analysis/pdf2xml/src/PDFDocXrce.cc:34
    #10 0x40943b in main /home/test/pdf2xml_analysis/pdf2xml/src/pdftoxml.cc:409
    #11 0x7f08688f582f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #12 0x403d28 in _start (/home/test/pdf2xml_analysis/pdf2xml/pdf2xml+0x403d28)

0x60200004999a is located 0 bytes to the right of 10-byte region [0x602000049990,0x60200004999a)
```

```
allocated by thread T0 here:
    #0 0x7f0869e58602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x4148c4 in TextPage::addAttributsNode(_xmlNode*, TextWord*, double&, double&, double&, double&, double&, double&)
/home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1389
    #2 0x417c7c in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1815
    #3 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
    #4 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
    #5 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __interceptor_vsprintf
Shadow bytes around the buggy address:
  0x0c04800012e0: fa fa 00 fa fa fa 00 03 fa fa fd fa fa fa fd fd
  0x0c04800012f0: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fd
  0x0c0480001300: fa fa 00 fa fa fa 00 00 fa fa 02 fa fa fa 00 02
  0x0c0480001310: fa fa 03 fa fa fa 07 fa fa fa 03 fa fa fa 05 fa
  0x0c0480001320: fa fa 04 fa fa fa 06 fa fa fa 04 fa fa fa 00 01
=>0x0c0480001330: fa fa 00[02]fa fa 00 fa fa fa 00 02 fa fa 00 fa
  0x0c0480001340: fa fa 00 00 fa fa 00 fa fa fa fd fa fa fa 00 fa
  0x0c0480001350: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa 06 fa
  0x0c0480001360: fa fa 03 fa fa fa fd fd fa fa fd fa fa fa fd fd
  0x0c0480001370: fa fa 06 fa fa fa 04 fa fa fa fd fd fa fa fd fa
  0x0c0480001380: fa fa fd fd fa fa 06 fa fa fa 05 fa fa fa 00 02
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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==57105==ABORTING

Function : TextPage::addAttributsNode
Type: heap-overflow
```

03-Unknow-pointer-dereference-TextPage-restoreState

```
$ ./pdf2xml 03-Unknow-pointer-dereference-TextPage-restoreState.pdf test.xml

Syntax Error (568381): Too few (0) args to 'y' operator
ASAN:SIGSEGV
=================================================================
==14321==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000041f38e bp 0x7fff22ae1510 sp 0x7fff22ae1500 T0)
    #0 0x41f38d in TextPage::restoreState(GfxState*) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:2765
    #1 0x429fe6 in XmlOutputDev::restoreState(GfxState*) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4333
    #2 0x48e639 in Gfx::drawForm(Object*, Dict*, double*, double*, int, int, GfxColorSpace*, int, int, int, Function*, GfxColor*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:4395
    #3 0x49321f in Gfx::drawAnnot(Object*, AnnotBorderStyle*, double, double, double, double)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:4738
    #4 0x476d85 in Annot::draw(Gfx*, int) /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Annot.cc:1039
    #5 0x45648b in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:381
    #6 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310
    #7 0x45740d in PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/PDFDoc.cc:398
    #8 0x407de8 in PDFDocXrce::displayPages(OutputDev*, _xmlNode*, int, int, double, double, int, int, int, int, int (*)(void*),
void*) /home/test/pdf2xml_analysis/pdf2xml/src/PDFDocXrce.cc:34
    #9 0x40943b in main /home/test/pdf2xml_analysis/pdf2xml/src/pdftoxml.cc:409
    #10 0x7f39d69bf82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #11 0x403d28 in _start (/home/test/pdf2xml_analysis/pdf2xml/pdf2xml+0x403d28)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:2765 TextPage::restoreState(GfxState*)
==14321==ABORTING

$ gdb ./pdf2xml ../../pdf2xml_out_tmin/crashes.2020-07-03-18\:59\:32/id:000024,sig:11,src:000004,op:flip1,pos:568370 test.xml

Excess command line arguments ignored. (test.xml)
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
```

```
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./pdf2xml...done.
"/home/test/pdf2xml_analysis/pdf2xml/../../pdf2xml_out_tmin/crashes.2020-07-03-
18:59:32/id:000024,sig:11,src:000004,op:flip1,pos:568370" is not a core dump: File format not recognized
(gdb) r ../../pdf2xml_out_tmin/crashes.2020-07-03-18\:59\:32/id:000024,sig:11,src:000004,op:flip1,pos:568370 test.xml
Starting program: /home/test/pdf2xml_analysis/pdf2xml/pdf2xml ../../pdf2xml_out_tmin/crashes.2020-07-03-
18\:59\:32/id:000024,sig:11,src:000004,op:flip1,pos:568370 test.xml
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Syntax Error (568381): Too few (0) args to 'y' operator

Program received signal SIGSEGV, Segmentation fault.
0x000000000041f38e in TextPage::restoreState (this=0x61500000b980, state=0x61700000f900) at
/home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:2765
2765            idCur = idStack.top();
(gdb) x/5i $rip
=> 0x41f38e <TextPage::restoreState(GfxState*)+54>:     movzbl (%rdx),%edx
   0x41f391 <TextPage::restoreState(GfxState*)+57>:     test   %dl,%dl
   0x41f393 <TextPage::restoreState(GfxState*)+59>:     setne  %sil
   0x41f397 <TextPage::restoreState(GfxState*)+63>:     mov    %rax,%rdi
   0x41f39a <TextPage::restoreState(GfxState*)+66>:     and    $0x7,%edi
(gdb) p/x $rdx
$1 = 0x17d7d7d857d75817
(gdb) x/gx $rdx
0x17d7d7d857d75817:     Cannot access memory at address 0x17d7d7d857d75817


Function : TextPage::restoreState
Type: unkown-pointer
```

04-Memory leaks-TextPage-testLinkedText.pdf

```
$ ./pdf2xml 04-Memory leaks-TextPage-testLinkedText.pdf test.xml
=================================================================
==82085==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 99000 byte(s) in 99 object(s) allocated from:
        #0 0x7f1554619602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
        #1 0x7f1553d2f735  (/usr/lib/x86_64-linux-gnu/libxml2.so.2+0x2e735)

Direct leak of 4850 byte(s) in 97 object(s) allocated from:
        #0 0x7f1554619602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
        #1 0x4156a9 in TextPage::testLinkedText(_xmlNode*, double, double, double, double)
/home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1473
        #2 0x41773d in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1764
        #3 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
        #4 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
        #5 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310

Direct leak of 3924 byte(s) in 97 object(s) allocated from:
        #0 0x7f1554619602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
        #1 0x417a6c in TextPage::dump(int, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1800
        #2 0x428ec5 in XmlOutputDev::endPage() /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4155
        #3 0x48e309 in Gfx::~Gfx() /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:591
        #4 0x45653e in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*), void*)
/home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Page.cc:310

Direct leak of 3316 byte(s) in 227 object(s) allocated from:
        #0 0x7f15545e330f in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x6230f)
        #1 0x40a476 in TextWord::TextWord(GfxState*, int, int, int, int, double, double, int, TextFontInfo*, double, int, int)
/home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:212
        #2 0x4125fc in TextPage::beginWord(GfxState*, double, double) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1160
        #3 0x4128c9 in TextPage::addChar(GfxState*, double, double, double, double, unsigned int, int, unsigned int*, int)
/home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:1178
        #4 0x429048 in XmlOutputDev::drawChar(GfxState*, double, double, double, double, double, double, unsigned int, int,
unsigned int*, int) /home/test/pdf2xml_analysis/pdf2xml/src/XmlOutputDev.cc:4172
        #5 0x4935b1 in Gfx::doShowText(GString*) /home/test/pdf2xml_analysis/pdf2xml/xpdf/xpdf/Gfx.cc:3646
```

05-Stack-buffer-overflow-XRef-getObjectStream.pdf

```
$ gdb ./pdf2xml

(gdb) r 05-Stack-buffer-overflow-XRef-getObjectStream.pdf test.xml
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Syntax Error (593163): Dictionary key must be a name object
Syntax Error (593170): Dictionary key must be a name object

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6e8c80b in ?? () from /usr/lib/x86_64-linux-gnu/libasan.so.2
(gdb) x/5i $rip
=> 0x7ffff6e8c80b:      mov    %ecx,0x8(%rsp)
0x7ffff6e8c80f: mov    %r8d,0x10(%rsp)
0x7ffff6e8c814: mov    (%rax),%eax
```

```
0x7ffff6e8c816: test   %eax,%eax
0x7ffff6e8c818: je     0x7ffff6e8d0a0
```