# NULL-pointer-dereference-TextPage-restoreState #10

Open **Aurorainfinity** opened this issue on Jul 5, 2020 · 0 comments

**Aurorainfinity** commented on Jul 5, 2020

$ gdb ./pdf2xml
(gdb) r 01-NULL-pointer-dereference-TextPage-restoreState test.xml
00-NULL-pointer-dereference-TextPage-restoreState.pdf

```
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  0x000000000049983b 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  0x00000000000499a4f in Gfx::go (this=this@entry=0x7a0140, topLevel=topLevel@entry=1) at /home/test/pdf2xml/xpdf/xpdf/Gfx.cc:709
#4  0x00000000000499e66 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  0x00000000000465f23 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  0x0000000000466ffb 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  0x000000000046707e 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
```

ref:
https://github.com/Aurorainfinity/Poc/tree/master/pdf2xml

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant