# segmemtation fault at xpdf-4.04/xpdf/AcroForm.cc:538

Post Reply | Search this topic... | 2 posts • Page 1 of 1

**ycdxsb**

## segmemtation fault at xpdf-4.04/xpdf/AcroForm.cc:538

Sat Jul 16, 2022 6:00 am

version:4.04
reproduce: pdftotext poc.pdf

CODE: SELECT ALL

```
pwndbg> bt
#0  0x000055555561d7c9 in gAtomicIncrement (counter=<error reading variable: Cannot access memory at
#1  0x000055555561d832 in Dict::incRef (this=0x5555557d1960) at /root/xpdf-4.04/xpdf/Dict.h:40
#2  0x000055555568a4d5 in Object::copy (this=0x5555557b7bc8, obj=0x7fffff7ff1b0) at /root/xpdf-4.04/x
#3  0x00005555556b2f47 in XRef::fetch (this=0x5555557b74e0, num=233, gen=0, obj=0x7fffff7ff1b0, recur
#4  0x000055555568a575 in Object::fetch (this=0x5555557cfaf8, xref=0x5555557b74e0, obj=0x7fffff7ff1b0
#5  0x000055555561d6b1 in Dict::lookup (this=0x5555557cebb0, key=0x5555556dd841 "Parent", obj=0x7ffff
#6  0x000055555568b126 in Object::dictLookup (this=0x7fffff7ff1c0, key=0x5555556dd841 "Parent", obj=0
#7  0x00005555555fad06 in AcroForm::scanField (this=0x5555557b6b60, fieldRef=0x7fffff7ff250) at /root
#8  0x00005555555fad9b in AcroForm::scanField (this=0x5555557b6b60, fieldRef=0x7fffff7ff2d0) at /root
#9  0x00005555555fad9b in AcroForm::scanField (this=0x5555557b6b60, fieldRef=0x7fffff7ff350) at /root
#10 0x00005555555fad9b in AcroForm::scanField (this=0x5555557b6b60, fieldRef=0x7fffff7ff3d0) at /root
#11 0x00005555555fad9b in AcroForm::scanField (this=0x5555557b6b60, fieldRef=0x7fffff7ff450) at /root
```

ATTACHMENTS

poc.pdf.zip
(30.31 KiB) Downloaded 140 times

**derekn**

## Re: segmemtation fault at xpdf-4.04/xpdf/AcroForm.cc:538

Mon Jul 18, 2022 8:37 pm

This is an object loop in the PDF structure. I'm working on a more robust loop detector for Xpdf 5.