SEGV_in_getObj #12

Open **Cvjark** opened this issue on Aug 7 · 0 comments

Cvjark commented on Aug 7 • edited

Hi, in the lastest version of this code [ps: commit id ffaf11c] I found something unusual.

crash sample

8id95_SEGV_in_getObj.zip

command to reproduce

```
./pdftops -q [crash sample] /dev/null
```

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==115957==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x000000689bd4 bp 0x0000957f8ba1 sp
0x7ffd52912760 T0)
==115957==The signal is caused by a READ memory access.
==115957==Hint: this fault was caused by a dereference of a high value address (see register
values below).  Disassemble the provided pc to learn which register was used.
    #0 0x689bd4 in Lexer::getObj(Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:132:16
    #1 0x6a8fc5 in Parser::Parser(XRef*, Lexer*, int) /home/bupt/Desktop/xpdf/xpdf/Parser.cc:33:10
    #2 0x581742 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:641:16
    #3 0x6a76a1 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:360:10
    #4 0x6d5f6e in PSOutputDev::checkPageSlice(Page*, double, double, int, int, int, int, int,
int, int, int, int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PSOutputDev.cc:3276:11
    #5 0x6a7172 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:328:13
    #6 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*),
void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
    #7 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27
    #8 0x6af9b4 in PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int,
int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:397:5
```

```
    #9 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
    #10 0x7f84f066ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #11 0x41d5d9 in _start (/home/bupt/Desktop/xpdf/xpdf/pdftops+0x41d5d9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:132:16 in
Lexer::getObj(Object*)
==115957==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant