

[New issue](#)
[Jump to bottom](#)

SEGV_in_getChar #5

Open Cvjark opened this issue on Aug 7 · 0 comments

Cvjark commented on Aug 7 • edited ▼

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

crash sample

[8id46_SEGV_in_getChar.zip](#)

command to reproduce

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

crash detail

```
AddressSanitizer:DEADLYSIGNAL
```

```
=====
```

```
==115845==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000750afe bp 0x0c40000003cc sp 0x7ffd6a600d80 T0)
```

```
==115845==The signal is caused by a READ memory access.
```

```
==115845==Hint: address points to the zero page.
```

```

#0 0x750afe in DCTStream::getChar() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2302:9
#1 0x6899e3 in Object::streamGetChar() /home/bupt/Desktop/xpdf/xpdf/.Object.h:288:20
#2 0x6899e3 in Lexer::getChar() /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:92:42
#3 0x6899e3 in Lexer::getObj(Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:124:14
#4 0x6a8fc5 in Parser::Parser(XRef*, Lexer*, int) /home/bupt/Desktop/xpdf/xpdf/Parser.cc:33:10
#5 0x581742 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:641:16
#6 0x6a76a1 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int, int, int (*) (void*), void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:360:10
#7 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
#8 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
#9 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*) (void*), void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
#10 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int (*) (void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27

```

```
#11 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
#12 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
#13 0x7f558fd59c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
#14 0x41d5d9 in _start (/home/bupt/Desktop/xpdf/xpdf/pdftops+0x41d5d9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2302:9 in
DCTStream::getChar()
==115845==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

