SEGV_in_readMCURow #9

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

8id69_SEGV_in_readMCURow.zip

command to reproduce

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

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==115909==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000751cdd bp
0x7fffab2f8a10 sp 0x7fffab2f8640 T0)
==115909==The signal is caused by a WRITE memory access.
==115909==Hint: address points to the zero page.
    #0 0x751cdd in DCTStream::readMCURow() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2403:23
    #1 0x750d6e in DCTStream::getChar() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2316:12
    #2 0x6899e3 in Object::streamGetChar() /home/bupt/Desktop/xpdf/xpdf/./Object.h:288:20
    #3 0x6899e3 in Lexer::getChar() /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:92:42
    #4 0x6899e3 in Lexer::getObj(Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:124:14
    #5 0x6a8fc5 in Parser::Parser(XRef*, Lexer*, int) /home/bupt/Desktop/xpdf/xpdf/Parser.cc:33:10
    #6 0x581742 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:641:16
    #7 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
    #8 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
    #9 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
    #10 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*),
void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
    #11 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
```

```
(*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27
    #12 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
    #13 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
    #14 0x7fabd9c46c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #15 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:2403:23 in
DCTStream::readMCURow()
==115909==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant