New issue

Jump to bottom

FPE_in_decodeImage #6

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

8id63_FPE_in_decodeImage.zip

command to reproduce

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

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==115861==ERROR: AddressSanitizer: FPE on unknown address 0x0000007476d3 (pc 0x0000007476d3 bp
0x7fff22d95b40 sp 0x7fff22d952c0 T0)
    #0 0x7476d3 in DCTStream::decodeImage() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2813:19
    #1 0x7402bb in DCTStream::reset() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2261:5
    #2 0x68912e in Object::streamReset() /home/bupt/Desktop/xpdf/xpdf/./Object.h:282:13
    #3 0x68912e in Lexer::Lexer(XRef*, Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:74:12
    #4 0x581714 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:641:33
    #5 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
    #6 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
    #7 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
    #8 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*),
void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
    #9 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27
    #10 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
    #11 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
```

```
    #12 0x7ffb8625dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #13 0x41d5d9 in _start (/home/bupt/Desktop/xpdf/xpdf/pdftops+0x41d5d9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2813:19 in
DCTStream::decodeImage()
==115861==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant