New issue

Jump to bottom

A Segmentation fault in InfoOutputDev.cc:880 #99

Open seviezhou opened this issue on Jul 31, 2020 · 0 comments

seviezhou commented on Jul 31, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), pdf2swf (latest master fad6c2)

Command line

./pdf2swf -qq -z -o /dev/null ./SEGV-type3D0-InfoOutputDev-880

Output

```
Segmentation fault (core dumped)
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==67223==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000018 (pc 0x55e7a871efe0 bp 0x0c1a000019b0 sp 0x7ffe4b1c6f00 T0)
    #0 0x55e7a871efdf in InfoOutputDev::type3D0(GfxState*, double, double) /home/seviezhou/swftools/lib/pdf/InfoOutputDev.cc:880
    #1 0x55e7a85c15e5 in Gfx::go(int) xpdf/Gfx.cc:584
    #2 0x55e7a85c2e9f in Gfx::display(Object*, int) xpdf/Gfx.cc:556
    #3 0x55e7a8561e20 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:317
    #4 0x55e7a8562d4a in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:266
    #5 0x55e7a84645af in pdf_open /home/seviezhou/swftools/lib/pdf/pdf.cc:542
    #6 0x55e7a82e67d5 in main /home/seviezhou/swftools/src/pdf2swf.c:737
    #7 0x7f02969f0b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x55e7a82eff09 in _start (/home/seviezhou/swftools/src/pdf2swf+0x17cf09)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/swftools/lib/pdf/InfoOutputDev.cc:880 InfoOutputDev::type3D0(GfxState*, double, double)
==67223==ABORTING
```

POC

SEGV-type3D0-InfoOutputDev-880.zip

Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant