New issue

Jump to bottom

A Segmentation fault in InfoOutputDev.cc:887 #105

Open seviezhou opened this issue on Aug 1, 2020 · 0 comments

seviezhou commented on Aug 1, 2020

System info

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

Command line

./pdf2swf -qq -z -o /dev/null ./SEGV-type3D1-InfoOutputDev-887

Output

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

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==10741==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000048 (pc 0x5653bc913184 bp 0x000000000007 sp 0x7fffd8dd2fd0 T0)
    #0 0x5653bc913183 in InfoOutputDev::type3D1(GfxState*, double, double, double, double, double, double) /home/seviezhou/swftools/lib/pdf/InfoOutputDev.cc:887
    #1 0x5653bc7b55e5 in Gfx::go(int) xpdf/Gfx.cc:584
    #2 0x5653bc7b6e9f in Gfx::display(Object*, int) xpdf/Gfx.cc:556
    #3 0x5653bc755e20 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:317
    #4 0x5653bc756d4a in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:266
    #5 0x5653bc6585af in pdf_open /home/seviezhou/swftools/lib/pdf/pdf.cc:542
    #6 0x5653bc4da7d5 in main /home/seviezhou/swftools/src/pdf2swf.c:737
    #7 0x7efd90625b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x5653bc4e3f09 in _start (/home/seviezhou/swftools/src/pdf2swf+0x17cf09)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/swftools/lib/pdf/InfoOutputDev.cc:887 InfoOutputDev::type3D1(GfxState*, double, double, double, double, double, double)
==10741==ABORTING
```

POC

SEGV-type3D1-InfoOutputDev-887.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