New issue

Jump to bottom

A SEGV in xpdf/GString.cc:173 #101

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-GString-GString-173

AddressSanitizer output

```
Error: Type 4 function isn't a stream
ASAN:SIGSEGV
=================================================================
==12533==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x56502776e723 bp 0xbebebebebebebebe sp 0x7ffd8b037888 T0)
    #0 0x56502776e722 in GString::~GString() xpdf/GString.cc:173
    #1 0x565027977b24 in PostScriptFunction::~PostScriptFunction() xpdf/Function.cc:1060
    #2 0x565027977c20 in PostScriptFunction::~PostScriptFunction() xpdf/Function.cc:1061
    #3 0x565027983f99 in Function::parse(Object*) xpdf/Function.cc:74
    #4 0x565027949ac9 in GfxRadialShading::parse(Dict*) xpdf/GfxState.cc:2220
    #5 0x56502795e0f9 in GfxShading::parse(Object*) xpdf/GfxState.cc:1691
    #6 0x56502795e668 in GfxShadingPattern::parse(Object*) xpdf/GfxState.cc:1588
    #7 0x56502795f147 in GfxPattern::parse(Object*) xpdf/GfxState.cc:1447
    #8 0x5650278bf347 in GfxResources::lookupPattern(char*) xpdf/Gfx.cc:388
    #9 0x5650278c8620 in Gfx::opSetFillColorN(Object*, int) xpdf/Gfx.cc:1248
    #10 0x5650278c35e5 in Gfx::go(int) xpdf/Gfx.cc:584
    #11 0x5650278c4e9f in Gfx::display(Object*, int) xpdf/Gfx.cc:556
    #12 0x565027863e20 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:317
    #13 0x565027864d4a in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:266
    #14 0x5650277665af in pdf_open /home/seviezhou/swftools/lib/pdf/pdf.cc:542
    #15 0x5650275e87d5 in main /home/seviezhou/swftools/src/pdf2swf.c:737
    #16 0x7f4cd0492b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #17 0x5650275f1f09 in _start (/home/seviezhou/swftools/src/pdf2swf+0x17cf09)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV xpdf/GString.cc:173 GString::~GString()
==12533==ABORTING
```

POC

SEGV-GString-GString-173.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