New issue

Jump to bottom

A Segmentation fault in textglyph.cpp:35:32 #5

Open seviezhou opened this issue on Aug 5, 2020 · 0 comments

seviezhou commented on Aug 5, 2020

System info

Ubuntu x86_64, clang 6.0, pdftools (latest master 7fe388)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

Command line

./src/pdftools -o /dev/null @@

Output

```
Segmentation fault
```

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==60075==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x00000054b869 bp 0x7ffe03342630 sp 0x7ffe033424d0 T0)
==60075==The signal is caused by a READ memory access.
==60075==Hint: address points to the zero page.
    #0 0x54b868 in Font::Size() /home/seviezhou/pdftools/src/semantic/font.cpp:45:12
    #1 0x58456b in TextGlyph::DoGlyph(Html*) /home/seviezhou/pdftools/src/glyphs/textglyph.cpp:35:32
    #2 0x582b99 in Glyph::Execute(Html*, Context*) /home/seviezhou/pdftools/src/glyphs/glyph.cpp:51:5
    #3 0x582dc0 in Glyph::Execute(Html*, Context*) /home/seviezhou/pdftools/src/glyphs/glyph.cpp:62:23
    #4 0x544b5f in Page::Execute(Html*) /home/seviezhou/pdftools/src/semantic/page.cpp:76:13
    #5 0x573216 in EPUB::GeneratePages() /home/seviezhou/pdftools/src/epub/epub.cpp:331:15
    #6 0x573aa8 in EPUB::Generate(Document*, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)
/home/seviezhou/pdftools/src/epub/epub.cpp:352:9
    #7 0x53cc3f in Converter::Convert() /home/seviezhou/pdftools/src/converter.cpp:86:27
    #8 0x51fc32 in main /home/seviezhou/pdftools/src/main.cpp:140:27
    #9 0x7fc2f3deb83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #10 0x41dc48 in _start (/home/seviezhou/pdftools/src/pdftools+0x41dc48)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/pdftools/src/semantic/font.cpp:45:12 in Font::Size()
==60075==ABORTING
```

POC

SEGV-DoGlyph-textglyph-35.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant