New issue

Jump to bottom

A Segmentation fault in analyze.cpp:509:50 #4

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
=================================================================
==17199==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000020 (pc 0x000000585c39 bp 0x7fffae8fbb10 sp 0x7fffae8fb3f0 T0)
==17199==The signal is caused by a READ memory access.
==17199==Hint: address points to the zero page.
    #0 0x585c38 in node::ObjNode::Value() const /home/seviezhou/pdftools/src/nodes/objnode.cpp:50:12
    #1 0x53469d in Analyze::GetStream(node::ObjNode*, std::__cxx11::basic_stringstream<char, std::char_traits<char>, std::allocator<char> >*)
/home/seviezhou/pdftools/src/analyze.cpp:509:50
    #2 0x536958 in Analyze::GetStream(node::ArrayNode*, std::__cxx11::basic_stringstream<char, std::char_traits<char>, std::allocator<char> >*)
/home/seviezhou/pdftools/src/analyze.cpp:502:13
    #3 0x531155 in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:645:21
    #4 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #5 0x52fa95 in Analyze::AnalyzeTree() /home/seviezhou/pdftools/src/analyze.cpp:383:9
    #6 0x53c283 in Converter::Convert() /home/seviezhou/pdftools/src/converter.cpp:62:36
    #7 0x51fc32 in main /home/seviezhou/pdftools/src/main.cpp:140:27
    #8 0x7ff7b20a083f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #9 0x41dc48 in _start (/home/seviezhou/pdftools/src/pdftools+0x41dc48)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/pdftools/src/nodes/objnode.cpp:50:12 in node::ObjNode::Value() const
==17199==ABORTING
```

POC

SEGV-GetStream-analyze-509.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant