New issue

Jump to bottom

# A Segmentation fault in analyze.cpp:422:1 #6

Open **seviezhou** opened this issue on Aug 6, 2020 · 0 comments

**seviezhou** commented on Aug 6, 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
=================================================================
==7714==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000058c806 bp 0x602000000358 sp 0x7ffceb03c2b0 T0)
==7714==The signal is caused by a READ memory access.
==7714==Hint: address points to the zero page.
    #0 0x58c805 in node::BDCNode::~BDCNode() /home/seviezhou/pdftools/src/nodes/bdcnode.cpp:34:9
    #1 0x58c805 in node::BDCNode::~BDCNode() /home/seviezhou/pdftools/src/nodes/bdcnode.cpp:31
    #2 0x58bf3a in node::RootNode::~RootNode() /home/seviezhou/pdftools/src/nodes/rootnode.cpp:33:9
    #3 0x58c13c in node::RootNode::~RootNode() /home/seviezhou/pdftools/src/nodes/rootnode.cpp:30:1
    #4 0x5514bf in parser::PageParser::~PageParser() /home/seviezhou/pdftools/src/parser/pageparser.cpp:42:9
    #5 0x53243c in Analyze::ProcessPage(int, int, std::__cxx11::basic_stringstream<char, std::char_traits<char>, std::allocator<char> >*, node::MapNode*, node::ArrayNode*)
/home/seviezhou/pdftools/src/analyze.cpp:422:1
    #6 0x531224 in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:648:37
    #7 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #8 0x52fa95 in Analyze::AnalyzeTree() /home/seviezhou/pdftools/src/analyze.cpp:383:9
    #9 0x53c283 in Converter::Convert() /home/seviezhou/pdftools/src/converter.cpp:62:36
    #10 0x51fc32 in main /home/seviezhou/pdftools/src/main.cpp:140:27
    #11 0x7f910538183f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #12 0x41dc48 in _start (/home/seviezhou/pdftools/src/pdftools+0x41dc48)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/pdftools/src/nodes/bdcnode.cpp:34:9 in node::BDCNode::~BDCNode()
==7714==ABORTING
```

## POC

SEGV-ProcessPage-analyze-422.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant