New issue

Jump to bottom

A Segmentation fault in analyze.cpp:74:55 #3

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
=================================================================
==73464==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000018 (pc 0x000000588dab bp 0x7ffd4c347190 sp 0x7ffd4c346bf0 T0)
==73464==The signal is caused by a READ memory access.
==73464==Hint: address points to the zero page.
    #0 0x588daa in std::_Rb_tree<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >, std::pair<std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const, node::TreeNode*>, std::_Select1st<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const, node::TreeNode*> >,
std::less<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const, node::TreeNode*> >::_M_begin() const /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_tree.h:748:29
    #1 0x588daa in std::_Rb_tree<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >, std::pair<std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const, node::TreeNode*>, std::_Select1st<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const, node::TreeNode*> >,
std::less<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const, node::TreeNode*> >::find(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&) const /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/stl_tree.h:2559
    #2 0x587d70 in std::map<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >, node::TreeNode*, std::less<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const, node::TreeNode*> >
>::find(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&) const /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/stl_map.h:1194:21
    #3 0x587d70 in node::MapNode::Get(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >) const /home/seviezhou/pdftools/src/nodes/mapnode.cpp:42
    #4 0x526839 in Analyze::AnalyzeXref() /home/seviezhou/pdftools/src/analyze.cpp:74:55
    #5 0x52f9a6 in Analyze::AnalyzeTree() /home/seviezhou/pdftools/src/analyze.cpp:373:5
    #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 0x7ffb5fda783f 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 /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_tree.h:748:29 in std::_Rb_tree<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const, node::TreeNode*>,
std::_Select1st<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const, node::TreeNode*> >, std::less<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const, node::TreeNode*> >
>::_M_begin() const
==73464==ABORTING
```

POC

SEGV-AnalyzeXref-analyze-74.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant