

New issue

[Jump to bottom](#)

SEGV in CoreFile.tcc:69 #766

🔒 Closed

CCWANG19 opened this issue on Aug 10 · 0 comments

Assignees



Labels

bug ELF

CCWANG19 commented on Aug 10 • edited ▾

version

latest master 365a16a

Build platform

Ubuntu 20.04.3 LTS (Linux 5.13.0-52-generic x86_64)

Build step

```
cmake -DLIEF_ASAN=ON ../
```

Run

```
./build/examples/c/elf_reader poc
```

[poc.zip](#)

Output

```
Can't access the content of section #0
Can't parse section #01
Binary doesn't have a program header
```

AddressSanitizer:DEADLYSIGNAL

=====

==3230843==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000020 (pc 0x559aec0a79de bp 0x0ffffef333808 sp 0x7fff7999c000 T0)

==3230843==The signal is caused by a WRITE memory access.

==3230843==Hint: address points to the zero page.

```
#0 0x559aec0a79dd in std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >::_M_length(unsigned long) /usr/include/c++/9/bits/basic_string.h:187
#1 0x559aec0a79dd in std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >::_M_set_length(unsigned long) /usr/include/c++/9/bits/basic_string.h:220
#2 0x559aec0a79dd in std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >::operator=(std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&&) /usr/include/c++/9/bits/basic_string.h:756
#3 0x559aec0a79dd in void LIEF::ELF::CoreFile::parse<LIEF::ELF::details::ELF32>()
/home/wcc/LIEF/src/ELF/NoteDetails/core/CoreFile.tcc:69
#4 0x559aec09aa70 in LIEF::ELF::CoreFile::parse()
/home/wcc/LIEF/src/ELF/NoteDetails/core/CoreFile.cpp:114
#5 0x559aec09aa8d in LIEF::ELF::CoreFile::make(LIEF::ELF::Note&)
/home/wcc/LIEF/src/ELF/NoteDetails/core/CoreFile.cpp:38
#6 0x559aebfdeb66 in LIEF::ELF::Note::details() /home/wcc/LIEF/src/ELF/Note.cpp:156
#7 0x559aebfe14ee in LIEF::ELF::Note::Note(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, LIEF::ELF::NOTE_TYPES_CORE,
std::vector<unsigned char, std::allocator<unsigned char> > const&, LIEF::ELF::Binary*)
/home/wcc/LIEF/src/ELF/Note.cpp:92
#8 0x559aebf183ac in std::_MakeUniq<LIEF::ELF::Note>::__single_object
std::make_unique<LIEF::ELF::Note, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >&, LIEF::ELF::NOTE_TYPES_CORE, std::vector<unsigned char,
std::allocator<unsigned char> >, LIEF::ELF::Binary*>(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >&, LIEF::ELF::NOTE_TYPES_CORE&&,
std::vector<unsigned char, std::allocator<unsigned char> >&&, LIEF::ELF::Binary*&&)
/usr/include/c++/9/bits/unique_ptr.h:857
#9 0x559aebf183ac in LIEF::ELF::Parser::parse_notes(unsigned long, unsigned long)
/home/wcc/LIEF/src/ELF/Parser.cpp:568
#10 0x559aebf8c11c in boost::leaf::result<LIEF::ok_t>
LIEF::ELF::Parser::parse_binary<LIEF::ELF::details::ELF32>() /home/wcc/LIEF/src/ELF/Parser.tcc:296
#11 0x559aebf1bad5 in LIEF::ELF::Parser::init(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&) /home/wcc/LIEF/src/ELF/Parser.cpp:323
#12 0x559aebf1bf8d in LIEF::ELF::Parser::parse(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, LIEF::ELF::DYN_SYM_COUNT_METHODS)
/home/wcc/LIEF/src/ELF/Parser.cpp:342
#13 0x559aebc1f3ae in elf_parse /home/wcc/LIEF/api/c/ELF/Binary.cpp:67
#14 0x559aebc1ce4f in main /home/wcc/LIEF/examples/c/elf_reader.c:16
#15 0x7f49b9b990b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
#16 0x559aebc1cc3d in _start (/home/wcc/LIEF/build/examples/c/elf_reader+0x281c3d)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /usr/include/c++/9/bits/basic_string.h:187 in
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>
>::_M_length(unsigned long)

==3230843==ABORTING



CCWANG19 assigned **romainthomas** on Aug 10



romainthomas added **bug** **ELF** labels on Aug 12



romainthomas closed this as completed in [ca93874](#) on Aug 13



romainthomas added a commit that referenced this issue 25 days ago



Fix [#766](#)

fe4d5b5

Assignees



romainthomas

Labels

bug

ELF

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

