SEGV in SegmentCommand.cpp:149 #764

Closed **CCWANG19** opened this issue on Aug 9 · 0 comments

Assignees 

Labels bug MachO Parser

CCWANG19 commented on Aug 9

version

```
latest master 5d1d643
```

Build platform

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

Build step

```
cmake .. -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -
DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address"
```

Run

```
./build/examples/c/macho_reader poc
```

poc.zip

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
```

```
==2360258==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000068 (pc 0x557d2bd89c98 bp
0x0ffffe483d3e sp 0x7ffff241e9b8 T0)
==2360258==The signal is caused by a READ memory access.
==2360258==Hint: address points to the zero page.
    #0 0x557d2bd89c97 in LIEF::MachO::SegmentCommand::file_offset() const
/home/wcc/LIEF/src/MachO/SegmentCommand.cpp:149
    #1 0x557d2bac147d in LIEF::MachO::Binary::segment_from_offset(unsigned long) const
/home/wcc/LIEF/src/MachO/Binary.cpp:541
    #2 0x557d2bbd3252 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse_dyldinfo_generic_bind<LIEF::MachO::details::MachO64>()
/home/wcc/LIEF/src/MachO/BinaryParser.tcc:1382
    #3 0x557d2bc40fc8 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse_dyldinfo_binds<LIEF::MachO::details::MachO64>()
/home/wcc/LIEF/src/MachO/BinaryParser.tcc:1356
    #4 0x557d2bc40fc8 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse<LIEF::MachO::details::MachO64>()
/home/wcc/LIEF/src/MachO/BinaryParser.tcc:113
    #5 0x557d2bb3ff6e in LIEF::MachO::BinaryParser::init_and_parse()
/home/wcc/LIEF/src/MachO/BinaryParser.cpp:145
    #6 0x557d2bb42ff9 in LIEF::MachO::BinaryParser::parse(std::unique_ptr<LIEF::BinaryStream,
std::default_delete<LIEF::BinaryStream> >, unsigned long, LIEF::MachO::ParserConfig const&)
/home/wcc/LIEF/src/MachO/BinaryParser.cpp:125
    #7 0x557d2b665077 in LIEF::MachO::Parser::build() /home/wcc/LIEF/src/MachO/Parser.cpp:174
    #8 0x557d2b667ce0 in LIEF::MachO::Parser::parse(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, LIEF::MachO::ParserConfig const&)
/home/wcc/LIEF/src/MachO/Parser.cpp:64
    #9 0x557d2b590706 in macho_parse /home/wcc/LIEF/api/c/MachO/Parser.cpp:27
    #10 0x557d2b555885 in main /home/wcc/LIEF/examples/c/macho_reader.c:148
    #11 0x7f9573af60b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #12 0x557d2b58f13d in _start (/home/wcc/LIEF/build/examples/c/macho_reader+0x31313d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/wcc/LIEF/src/MachO/SegmentCommand.cpp:149 in
LIEF::MachO::SegmentCommand::file_offset() const
==2360258==ABORTING
```

CCWANG19 assigned **romainthomas** on Aug 9

romainthomas added bug MachO Parser labels on Aug 10

romainthomas closed this as completed in `7acf0bc` on Aug 10

---

romainthomas added a commit that referenced this issue 25 days ago

`Resolve #764` `b891d9d`

Assignees

 romainthomas

Labels

bug MachO Parser

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants