

[New issue](#)[Jump to bottom](#)

SEGV in LIEF::MachO::BinaryParser::init_and_parse at MachO/BinaryParser.cpp:141 #781

✓ Closed

bladchan opened this issue on Sep 11 · 0 comments

Assignees



Labels

[bug](#) [MachO](#) [Parser](#)

bladchan commented on Sep 11

Describe the bug

A bad macho file which can lead `LIEF::MachO::Parser::parse()` to segmentation fault.

Poc is here: [poc.zip](#)

To Reproduce

1. Build the whole project with **ASAN**
2. Drive program (compile it with **ASAN** too):

```
// read_mecho.c
#include <LIEF/LIEF.hpp>

int main(int argc, char** argv){

    if(argc != 2) return 0;

    try {
        std::unique_ptr<LIEF::MachO::FatBinary> macho = LIEF::MachO::Parser::parse(argv[1]);
    } catch (const LIEF::exception& err) {
        std::cerr << err.what() << std::endl;
    }

    return 0;
}
```

3. Run Poc:

```
$ ./read_macho ./poc.bin
```

Expected behavior

Parse the Mach-O file without segmentation fault because segmentation fault can cause a Denial of Service (Dos).

Environment (please complete the following information):

- System and Version : Ubuntu 20.04 + gcc 9.4.0
- Target format : **Mach-O**
- LIEF commit version: [ad81191](#)

Additional context

ASAN says:

```
ubuntu@ubuntu:~/test/LIEF/fuzz$ ./read_macho poc.bin
Segment __LINKEDIT: content corrupted!
nlist[0].str_idx seems corrupted (0x24000001)
nlist[1].str_idx seems corrupted (0x24000000)
.....
nlist[354].str_idx seems corrupted (0x5b000001)
nlist[355].str_idx seems corrupted (0x5f000001)
AddressSanitizer:DEADLYSIGNAL
=====
==391961==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x5584fa6b0158 bp
0x7ffe8bbdaaa0 sp 0x7ffe8bbdaa00 T0)
==391961==The signal is caused by a WRITE memory access.
==391961==Hint: address points to the zero page.
#0 0x5584fa6b0157 in LIEF::MachO::BinaryParser::init_and_parse()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.cpp:141
#1 0x5584fa6e779d in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse_load_commands<LIEF::MachO::details::Mach032>()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.tcc:894
#2 0x5584fa6bee61 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse<LIEF::MachO::details::Mach032>()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.tcc:90
#3 0x5584fa6b0348 in LIEF::MachO::BinaryParser::init_and_parse()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.cpp:145
#4 0x5584fa6afab0 in LIEF::MachO::BinaryParser::parse(std::unique_ptr<LIEF::BinaryStream,
std::default_delete<LIEF::BinaryStream> >, unsigned long, LIEF::MachO::ParserConfig const&)
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.cpp:125
#5 0x5584f9f39c01 in LIEF::MachO::Parser::build()
/home/ubuntu/test/LIEF/src/MachO/Parser.cpp:174
#6 0x5584f9f36995 in LIEF::MachO::Parser::parse(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, LIEF::MachO::ParserConfig const&)
/home/ubuntu/test/LIEF/src/MachO/Parser.cpp:64
#7 0x5584f9da1923 in main /home/ubuntu/test/LIEF/fuzz/read_macho.c:8
#8 0x7f982e960082 in __libc_start_main ../csu/libc-start.c:308
#9 0x5584f9da155d in _start (/home/ubuntu/test/LIEF/fuzz/read_macho+0x33055d)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /home/ubuntu/test/LIEF/src/MachO/BinaryParser.cpp:141 in


```
LIEF::MachO::BinaryParser::init_and_parse()  
==391961==ABORTING
```

Hope that helps!

  **bladchan** assigned **romainthomas** on Sep 11

  **romainthomas** added **bug** **MachO** **Parser** labels on Sep 11

 **romainthomas** closed this as completed in [fde2c48](#) on Sep 12

 **romainthomas** added a commit that referenced this issue 25 days ago

 **Fix** [#781](#)

db9df0b

Assignees

 **romainthomas**

Labels

bug **MachO** **Parser**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

