Heap-buffer-overflow in LIEF::MachO::BinaryParser::parse_dyldinfo_generic_bind at MachO/BinaryParser.tcc:1629 #782

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 a heap-buffer-overflow(read) issue.
Poc here :
poc1.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 ./poc1.bin
```

Expected behavior
The code snippet where the issue happened should avoid the out-bounds read operation.

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 poc1.bin
nlist[0].str_idx seems corrupted (0xaf000000)
nlist[1].str_idx seems corrupted (0xaf000000)
......
nlist[355].str_idx seems corrupted (0x3d000001)
Indirect symbol index is out of range (1493172225 vs max sym: 356)
Wrong index: 4
Wrong index: 4
Wrong index: 4
Wrong index: 4
Wrong index: 4
Wrong index: 4
Wrong index: 4
Wrong index: 4
Wrong index: 4
=================================================================
==502744==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000420 at pc
0x55b43d8d9b42 bp 0x7ffe61a9cf10 sp 0x7ffe61a9cf00
READ of size 8 at 0x603000000420 thread T0
    #0 0x55b43d8d9b41 in std::enable_if<std::is_pointer<LIEF::MachO::SegmentCommand*>::value,
LIEF::MachO::SegmentCommand&>::type LIEF::ref_iterator<std::vector<LIEF::MachO::SegmentCommand*,
std::allocator<LIEF::MachO::SegmentCommand*> >&, LIEF::MachO::SegmentCommand*,
__gnu_cxx::__normal_iterator<LIEF::MachO::SegmentCommand**,
std::vector<LIEF::MachO::SegmentCommand*, std::allocator<LIEF::MachO::SegmentCommand*> > >
>::operator*<LIEF::MachO::SegmentCommand*>() const
/home/ubuntu/test/LIEF/include/LIEF/iterators.hpp:233
    #1 0x55b43d8bf315 in LIEF::ref_iterator<std::vector<LIEF::MachO::SegmentCommand*,
std::allocator<LIEF::MachO::SegmentCommand*> >&, LIEF::MachO::SegmentCommand*,
__gnu_cxx::__normal_iterator<LIEF::MachO::SegmentCommand**,
std::vector<LIEF::MachO::SegmentCommand*, std::allocator<LIEF::MachO::SegmentCommand*> > >
>::operator*() /home/ubuntu/test/LIEF/include/LIEF/iterators.hpp:226
    #2 0x55b43d892a91 in LIEF::ref_iterator<std::vector<LIEF::MachO::SegmentCommand*,
std::allocator<LIEF::MachO::SegmentCommand*> >&, LIEF::MachO::SegmentCommand*,
__gnu_cxx::__normal_iterator<LIEF::MachO::SegmentCommand**,
std::vector<LIEF::MachO::SegmentCommand*, std::allocator<LIEF::MachO::SegmentCommand*> > >
>::operator[](unsigned long) const /home/ubuntu/test/LIEF/include/LIEF/iterators.hpp:146
```

```
    #3 0x55b43d858628 in LIEF::ref_iterator<std::vector<LIEF::MachO::SegmentCommand*,
std::allocator<LIEF::MachO::SegmentCommand*> >&, LIEF::MachO::SegmentCommand*,
__gnu_cxx::__normal_iterator<LIEF::MachO::SegmentCommand**,
std::vector<LIEF::MachO::SegmentCommand*, std::allocator<LIEF::MachO::SegmentCommand*> > >
>::operator[](unsigned long) /home/ubuntu/test/LIEF/include/LIEF/iterators.hpp:133
    #4 0x55b43d8644a2 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse_dyldinfo_generic_bind<LIEF::MachO::details::MachO32>()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.tcc:1629
    #5 0x55b43d831a79 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse_dyldinfo_binds<LIEF::MachO::details::MachO32>()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.tcc:1357
    #6 0x55b43d801735 in boost::leaf::result<LIEF::ok_t>
LIEF::MachO::BinaryParser::parse<LIEF::MachO::details::MachO32>()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.tcc:113
    #7 0x55b43d7f2348 in LIEF::MachO::BinaryParser::init_and_parse()
/home/ubuntu/test/LIEF/src/MachO/BinaryParser.cpp:145
    #8 0x55b43d7f1ab0 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
    #9 0x55b43d07bc01 in LIEF::MachO::Parser::build()
/home/ubuntu/test/LIEF/src/MachO/Parser.cpp:174
    #10 0x55b43d078995 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
    #11 0x55b43cee3923 in main /home/ubuntu/test/LIEF/fuzz/read_macho.c:8
    #12 0x7f2be6489082 in __libc_start_main ../csu/libc-start.c:308
    #13 0x55b43cee355d in _start (/home/ubuntu/test/LIEF/fuzz/read_macho+0x33055d)

0x603000000420 is located 0 bytes to the right of 32-byte region [0x603000000400,0x603000000420)
allocated by thread T0 here:
    #0 0x7f2be6ab2587 in operator new(unsigned long)
../../../../src/libsanitizer/asan/asan_new_delete.cc:104
    #1 0x55b43d7d7c50 in __gnu_cxx::new_allocator<LIEF::MachO::SegmentCommand*>::allocate(unsigned
long, void const*) /usr/include/c++/9/ext/new_allocator.h:114
    #2 0xfffcc353843  (<unknown module>)
    #3 0x7ffe61a9deef  ([stack]+0x1deef)

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/ubuntu/test/LIEF/include/LIEF/iterators.hpp:233 in
std::enable_if<std::is_pointer<LIEF::MachO::SegmentCommand*>::value,
LIEF::MachO::SegmentCommand&>::type LIEF::ref_iterator<std::vector<LIEF::MachO::SegmentCommand*,
std::allocator<LIEF::MachO::SegmentCommand*> >&, LIEF::MachO::SegmentCommand*,
__gnu_cxx::__normal_iterator<LIEF::MachO::SegmentCommand**,
std::vector<LIEF::MachO::SegmentCommand*, std::allocator<LIEF::MachO::SegmentCommand*> > >
>::operator*<LIEF::MachO::SegmentCommand*>() const
Shadow bytes around the buggy address:
  0x0c067fff8030: fa fa 00 00 01 fa fa fa 00 00 01 fa fa fa fd fd
  0x0c067fff8040: fd fd fa fa fd fd fd fd fa fa 00 00 01 fa fa fa
  0x0c067fff8050: 00 00 01 fa fa fa 00 00 01 fa fa fa 00 00 01 fa
  0x0c067fff8060: fa fa 00 00 01 fa fa fa 00 00 01 fa fa fa 00 00
  0x0c067fff8070: 01 fa fa fa 00 00 01 fa fa fa 00 00 01 fa fa fa
=>0x0c067fff8080: 00 00 00 00[fa]fa 00 00 01 fa fa fa 00 00 01 fa
  0x0c067fff8090: fa fa 00 00 01 fa fa fa 00 00 01 fa fa fa 00 00
  0x0c067fff80a0: 01 fa fa fa 00 00 01 fa fa fa fd fd fd fd fa fa
  0x0c067fff80b0: 00 00 01 fa fa fa 00 00 01 fa fa fa 00 00 01 fa
  0x0c067fff80c0: fa fa 00 00 01 fa fa fa 00 00 01 fa fa fa 00 00
  0x0c067fff80d0: 01 fa fa fa 00 00 01 fa fa fa 00 00 01 fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==502744==ABORTING
```

bladchan assigned **romainthomas** on Sep 11

romainthomas added bug MachO Parser labels on Sep 11

romainthomas closed this as completed in 98d3392 on Sep 12

romainthomas added a commit that referenced this issue 25 days ago

Fix #782 8bd685c

Assignees

romainthomas

Labels

bug MachO Parser

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants