heap-buffer-overflow in macho_reader.c #767

Closed **CCWANG19** opened this issue on Aug 10 · 1 comment

Assignees 

Labels bug MachO

CCWANG19 commented on Aug 10

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/macho_reader poc
```

poc.zip

Output

```
Can't read the state data
Can't read the raw data of the load command
Binary Name: poc
```

```
Header
========
Magic: 0xcefaedfe
CPU Type: ARM64
CPU SubType: 0x0
File type: OBJECT
Number of commands: 0x13a
Commands size: 0x0
flags: 0x0
reserved: 0x0
Commands
========
THREAD               0x4040000f 0x00001c
=================================================================
==3241437==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000152 at pc
0x555c3f7df416 bp 0x7ffc25ef7040 sp 0x7ffc25ef7030
READ of size 1 at 0x602000000152 thread T0
    #0 0x555c3f7df415 in print_binary /home/wcc/LIEF/examples/c/macho_reader.c:39
    #1 0x555c3f7dff11 in main /home/wcc/LIEF/examples/c/macho_reader.c:150
    #2 0x7fe3286cb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #3 0x555c3f7debfd in _start (/home/wcc/LIEF/build/examples/c/macho_reader+0x280bfd)

0x602000000152 is located 1 bytes to the right of 1-byte region [0x602000000150,0x602000000151)
allocated by thread T0 here:
    #0 0x7fe328cf2808 in __interceptor_malloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cc:144
    #1 0x555c3f8e3d36 in LIEF::MachO::init_c_commands(Macho_Binary_t*, LIEF::MachO::Binary*)
/home/wcc/LIEF/api/c/MachO/LoadCommand.cpp:31

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/wcc/LIEF/examples/c/macho_reader.c:39 in
print_binary
Shadow bytes around the buggy address:
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 00 00 fa fa fd fa fa fa 00 00 fa fa 00 fa
  0x0c047fff8010: fa fa fd fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
=>0x0c047fff8020: fa fa 00 00 fa fa 00 00 fa fa[01]fa fa fa 00 fa
  0x0c047fff8030: fa fa 00 fa fa fa 00 fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa 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
==3241437==ABORTING
```

CCWANG19 assigned **romainthomas** on Aug 10

romainthomas added bug MachO labels on Aug 12

romainthomas closed this as completed in `0033b63` on Aug 13

---

romainthomas commented on Aug 13 — Member

Thank you again for reporting these issues!

romainthomas added a commit that referenced this issue 25 days ago

`Resolve #767` `20cde42`

Assignees

romainthomas

Labels

bug MachO

Projects

None yet

Milestone

No milestone

Development

Development

No branches or pull requests

2 participants