A heap overflow in pe_reader.c:133 (not issue in the library) #449

Closed **seviezhou** opened this issue on Aug 7, 2020 · 1 comment

Assignees

Labels **API** bug PE

seviezhou commented on Aug 7, 2020

System info

Ubuntu x86_64, gcc, pe_reader (latest master 4bbe410)

Configure

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

Command line

./build/examples/c/pe_reader @@

AddressSanitizer output

```
=================================================================
==64198==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000ea12 at pc 0x00000041167a bp 0x7ffeab862260 sp 0x7ffeab862250
READ of size 1 at 0x60200000ea12 thread T0
    #0 0x411679 in main /home/seviezhou/lief/examples/c/pe_reader.c:133
    #1 0x7f70317d283f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #2 0x4212d8 in _start (/home/seviezhou/experiment-3/AlphaFuzz-lief/test/pe_reader+0x4212d8)

0x60200000ea12 is located 1 bytes to the right of 1-byte region [0x60200000ea10,0x60200000ea11)
allocated by thread T0 here:
    #0 0x7f7032518602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x42585f in LIEF::PE::init_c_sections(Pe_Binary_t*, LIEF::PE::Binary*) /home/seviezhou/lief/api/c/PE/Section.cpp:31

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/lief/examples/c/pe_reader.c:133 main
Shadow bytes around the buggy address:
  0x0c047fff9cf0: fa fa fa fa fa fa 00 00 fa fa 00 fa fa fa 00 fa
  0x0c047fff9d00: fa fa 00 fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
  0x0c047fff9d10: fa fa 00 fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
  0x0c047fff9d20: fa fa 00 fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
  0x0c047fff9d30: fa fa 00 fa fa fa 01 fa fa fa 01 fa fa fa 01 fa
=>0x0c047fff9d40: fa fa[01]fa fa fa 01 fa fa fa 01 fa fa fa fd fd
  0x0c047fff9d50: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff9d60: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff9d70: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa fd fd
  0x0c047fff9d80: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff9d90: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==64198==ABORTING
```

POC

heap-overflow-main-pe_reader-133.zip

seviezhou assigned **romainthomas** on Aug 7, 2020

romainthomas added bug PE **API** labels on Aug 27, 2020

romainthomas commented on Aug 27, 2020 Member

Done with `19e0675`

romainthomas closed this as completed on Aug 27, 2020

Assignees

romainthomas

Labels

API bug PE

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants