New issue

Jump to bottom

Stack Buffer Overflow in mysofa2json #96

Closed **fuzzme-ops** opened this issue on Jan 10, 2020 · 9 comments

fuzzme-ops commented on Jan 10, 2020

We found Stack Buffer Overflow in mysofa2json binary and mysofa2json is complied with clang enabling ASAN.

Machine Setup

```
Machine : Ubuntu 16.04.3 LTS
gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.11)
Commit : be7ac15
Command : mysofa2json POC
```

POC : POC.zip

ASAN Output

```
fuzzme@fuzz:~/victim/libmysofa/src$ ./mysofa2json POC
=================================================================
==6267==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffffee4cd50 at pc 0x000000462551 bp 0x7ffffee4cc20 sp 0x7ffffee4c3d0
WRITE of size 20 at 0x7ffffee4cd50 thread T0
    #0 0x462550 in __interceptor_vsprintf (/home/fuzzme/victim/libmysofa/src/mysofa2json+0x462550)
    #1 0x462682 in __interceptor_sprintf (/home/fuzzme/victim/libmysofa/src/mysofa2json+0x462682)
    #2 0x4f77d8 in readDataVar /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:555:4
    #3 0x4f7d7a in readDataDim /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:589:17
    #4 0x4f935b in readData /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:602:9
    #5 0x4f935b in readOHDRHeaderMessageAttribute /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:706
    #6 0x4f935b in readOHDRmessages /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:822
    #7 0x4fa0d4 in readOCHK /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:865:8
    #8 0x4fa0d4 in readOHDRHeaderMessageContinue /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:631
    #9 0x4fa0d4 in readOHDRmessages /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:826
    #10 0x4f8326 in dataobjectRead /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:913:8
    #11 0x502dcf in directblockRead /home/fuzzme/victim/libmysofa/src/hdf/fractalhead.c:206:10
    #12 0x500fac in fractalheapRead /home/fuzzme/victim/libmysofa/src/hdf/fractalhead.c:457:10
    #13 0x4f850a in dataobjectRead /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:937:9
    #14 0x4f6f4e in superblockRead /home/fuzzme/victim/libmysofa/src/hdf/superblock.c:83:9
    #15 0x4ed5ad in mysofa_load /home/fuzzme/victim/libmysofa/src/hrtf/reader.c:249:9
    #16 0x4eafa6 in main /home/fuzzme/victim/libmysofa/src/tests/sofa2json.c:24:9
    #17 0x7efc6be5d82f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #18 0x419838 in _start (/home/fuzzme/victim/libmysofa/src/mysofa2json+0x419838)

Address 0x7ffffee4cd50 is located in stack of thread T0 at offset 48 in frame
    #0 0x4f717f in readDataVar /home/fuzzme/victim/libmysofa/src/hdf/dataobject.c:497

  This frame has 2 object(s):
    [32, 48) 'number'
    [64, 72) 'dataobject' <== Memory access at offset 48 partially underflows this variable
SUMMARY: AddressSanitizer: stack-buffer-overflow (/home/fuzzme/victim/libmysofa/src/mysofa2json+0x462550) in __interceptor_vsprintf
Shadow bytes around the buggy address:
  0x10007fdc1950: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc1960: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc1970: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc1980: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc1990: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10007fdc19a0: 00 00 00 00 f1 f1 f1 f1 00 00[f2]f2 00 f3 f3 f3
  0x10007fdc19b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc19c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc19d0: 00 00 00 00 f1 f1 f1 f1 04 f2 00 00 00 00 00 00
  0x10007fdc19e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007fdc19f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==6267==ABORTING
```

hoene commented on Jan 10, 2020 Owner

I was testing the file with
"gcc (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0" and "Ubuntu 18.04.3 LTS"
and the result was "Error reading file POC. Error code: 10000".
Are you sure that you use the latest version?

fuzzme-ops commented on Jan 10, 2020 Author

Yes, I downloaded the latest release (`be7ac15`) and compiled using CC=afl-clang-fast CXX=afl-clang-fast++ on Ubuntu 5.4.0-6ubuntu1~16.04.11

hoene commented on Jan 10, 2020 • edited Owner

Description: Ubuntu 16.04.6 LTS
gcc (Ubuntu 5.4.0-6ubuntu1~16.04.12) 5.4.0 20160609
works.

Description: Ubuntu 14.04.5 LTS
gcc (Ubuntu 4.8.4-2ubuntu1~14.04.4) 4.8.4
works.

Both using the default build flags.

May you provide a fix? May you have to set in src/hdf/fractalhead.c around line 36 the 10 to a lower value?

fuzzme-ops commented on Jan 10, 2020 Author

I complied the latest release (`be7ac15`) with gcc and tried parsing the file, got error 10000 or -1 (for some files). But I get the crash for clang enabled code with ASAN.

I am not currently aware of the fix. I didnt change any values in src/hdf/fractalhead.c.

fuzzme-ops commented on Jan 11, 2020 Author

@hoene Can you try the attached POC file ? It gives Segmentation fault for mysofa2json compiled with gcc.

POC : POC.zip

hoene commented on Jan 11, 2020 • edited by umlaeute Owner

Yes, I will do. Thank you

hoene commented on Jan 11, 2020 • edited Owner

Thank you for the new file as I did not need to install ASAN.
The latest commit `c31120a` fixed the issue with the second file.

fuzzme-ops commented on Jan 11, 2020 Author

@hoene I verified the new release `c31120a` and reported bug can closed.

fuzzme-ops closed this as completed on Jan 11, 2020

hoene commented on Jan 11, 2020 Owner

Thank you.

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants