New issue

Jump to bottom

Stack buffer overflow in readDataVar #136

Closed cve-reporting opened this issue on Aug 26, 2020 · 2 comments

cve-reporting commented on Aug 26, 2020 • edited

Incorrect use of sprintf on a too small buffer leads to a stack buffer overflow by 4 bytes in dataobject.c:806.
This can lead to overwriting the next variable on the stack and logic errors in the application or crash in case of strong stack protection.

GDB stacktrace:
#10 0x00000000004123ce in sprintf (__fmt=0x442844 "REF%08lX", __s=0x7fffffffcab0 "REF170000000000") at /usr/include/x86_64-linux-gnu/bits/stdio2.h:33
#11 readDataVar (reader=reader@entry=0x7fffffffd140, data=data@entry=0x7fffffffcb80, dt=dt@entry=0x7fffffffcb94, ds=ds@entry=0x7fffffffcbb0)
at libmysofa-master/src/hdf/dataobject.c:806
#12 0x0000000000412c4b in readDataDim (reader=0x7fffffffd140, da=0x7fffffffcb80, dt=0x7fffffffcb94, ds=0x7fffffffcbb0, dim=dim@entry=0)
at libmysofa-master/src/hdf/dataobject.c:843
#13 0x0000000000412dc4 in readData (reader=reader@entry=0x7fffffffd140, da=da@entry=0x7fffffffcb80, dt=dt@entry=0x7fffffffcb94, ds=ds@entry=0x7fffffffcbb0)
at libmysofa-master/src/hdf/dataobject.c:856
#14 0x0000000000413aa7 in readOHDRHeaderMessageAttribute (reader=reader@entry=0x7fffffffd140, dataobject=0x61700000f588)
at libmysofa-master/src/hdf/dataobject.c:999
#15 0x0000000000414517 in readOHDRmessages (reader=reader@entry=0x7fffffffd140, dataobject=dataobject@entry=0x61700000f588, end_of_messages=end_of_messages@entry=13017)
at libmysofa-master/src/hdf/dataobject.c:1120
#16 0x00000000004176e5 in readOCHK (end=13021, dataobject=, reader=0x7fffffffd140) at libmysofa-master/src/hdf/dataobject.c:1162
#17 readOHDRHeaderMessageContinue (dataobject=, reader=0x7fffffffd140) at libmysofa-master/src/hdf/dataobject.c:890
#18 readOHDRmessages (reader=reader@entry=0x7fffffffd140, dataobject=dataobject@entry=0x61700000f588, end_of_messages=6851)
at libmysofa-master/src/hdf/dataobject.c:1124
#19 0x00000000004183e7 in dataobjectRead (reader=reader@entry=0x7fffffffd140, dataobject=dataobject@entry=0x61700000f588, name=name@entry=0x60200000ebd0 "ListenerView")
at libmysofa-master/src/hdf/dataobject.c:1211
#20 0x0000000000041d000 in directblockRead (reader=reader@entry=0x7fffffffd140, fractalheap=fractalheap@entry=0x7fffffffd290, dataobject=0x7fffffffd178, dataobject=0x7fffffffd178)
at libmysofa-master/src/hdf/fractalhead.c:238
#21 0x00000000004205c9 in fractalheapRead (reader=reader@entry=0x7fffffffd140, dataobject=dataobject@entry=0x7fffffffd178, fractalheap=fractalheap@entry=0x7fffffffd290)
at libmysofa-master/src/hdf/fractalhead.c:638
#22 0x00000000004187ef in dataobjectRead (reader=reader@entry=0x7fffffffd140, dataobject=dataobject@entry=0x7fffffffd178, name=name@entry=0x0)
at libmysofa-master/src/hdf/dataobject.c:1236
#23 0x000000000040ebde in superblockRead2or3 (reader=reader@entry=0x7fffffffd140, superblock=superblock@entry=0x7fffffffd150)
at libmysofa-master/src/hdf/superblock.c:64
#24 0x000000000040f6ab in superblockRead (reader=reader@entry=0x7fffffffd140, superblock=superblock@entry=0x7fffffffd150)
at libmysofa-master/src/hdf/superblock.c:170
#25 0x000000000040bb6c in mysofa_load (filename=filename@entry=0x7fffffffdb17 "crash_003_readDataVar_555.hdf", err=err@entry=0x7fffffffd540)
at libmysofa-master/src/hrtf/reader.c:305
#26 0x0000000000406d89 in mysofa_open_default (neighbor_radius_step=0.00999999978, neighbor_angle_step=0.5, applyNorm=true, err=0x7fffffffd540, filterlength=0x7fffffffd500,
samplerate=, filename=0x7fffffffdb17 "crash_003_readDataVar.hdf")
at libmysofa-master/src/hrtf/easy.c:37
#27 mysofa_open (filename=0x7fffffffdb17 "crash_003_readDataVar.hdf", samplerate=samplerate@entry=48000,
filterlength=filterlength@entry=0x7fffffffd500, err=err@entry=0x7fffffffd540) at libmysofa-master/src/hrtf/easy.c:86
#28 0x00000000004022d5 in main (argc=2, argv=0x7fffffffd698) at test_libmysofa.c:116

File triggering crash with ASAN (unzip before test):
crash_003_readDataVar.zip

Code snippet for reproduction:

```
int filter_length;
int err;
struct MYSOFA_EASY *easy = NULL;
easy = mysofa_open(filename, 48000, &filter_length, &err);
printf("Result: %p err: %d\n", easy, err);
mysofa_close(easy);
```

Solution:
Make the number buffer larger, use snprintf with the size of the number buffer and check the value returned by snprintf!

hoene commented on Nov 28, 2020 Owner

fixed with #146

hoene closed this as completed on Nov 28, 2020

abergmann commented on Feb 9, 2021

CVE-2020-36152 was assigned to this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants