hoene / libmysofa Public

<> Code ⊙ Issues 3 Pull requests ⊙ Actions Security Insights

New issue

Jump to bottom

NULL pointer dereference in verifyAttribute #138

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

cve-reporting commented on Aug 26, 2020

Opening maliciously crafted file with mysofa_open leads to crash of the application.
NULL pointer dereference in verifyAttribute (tools.c:26) on variable attr->value causes segmentation fault.

Message from gdb:

> Program received signal SIGSEGV, Segmentation fault.
> __strcmp_sse2_unaligned () at ../sysdeps/x86_64/multiarch/strcmp-sse2-unaligned.S:32

AddressSanitizer report on crash:
ASAN:SIGSEGV
==13017==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f777bf6b05e bp 0x7fff17798270 sp 0x7fff17797a00 T0)
#0 0x7f777bf6b05d (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x4705d)
#1 0x426747 in verifyAttribute libmysofa-master/src/hrtf/tools.c:26
#2 0x435b37 in mysofa_loudness libmysofa-master/src/hrtf/loudness.c:24
#3 0x406e97 in mysofa_open_default libmysofa-master/src/hrtf/easy.c:56
#4 0x406e97 in mysofa_open libmysofa-master/src/hrtf/easy.c:86
#5 0x4022d4 in main libmysofa-master/test_libmysofa.c:116
#6 0x7f777b65782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#7 0x402b48 in _start (libmysofa-master/test_libmysofa_asan.exe+0x402b48)

File triggering crash (unzip before test):
crash_004_verifyAttribute.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);
```

Affected versions:

- master (2020-08-26)
- 1.1
  (earlier versions have not been tested yet)

hoene mentioned this issue on Nov 28, 2020

Issue 138 zero m #145

Merged

hoene commented on Nov 28, 2020 Owner

fixed and merged

hoene closed this as completed on Nov 28, 2020

abergmann commented on Feb 9, 2021

CVE-2020-36148 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