New issue

Jump to bottom

NULL pointer dereference in changeAttribute #137

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 changeAttribute (tools.c:37) 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
==12754==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fec7bf0105e bp 0x7ffee7ed2090 sp 0x7ffee7ed1820 T0)
#0 0x7fec7bf0105d (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x4705d)
#1 0x4269d6 in changeAttribute libmysofa-master/src/hrtf/tools.c:37
#2 0x424dc9 in convertArray2 libmysofa-master/src/hrtf/spherical.c:27
#3 0x424dc9 in mysofa_tocartesian libmysofa-master/src/hrtf/spherical.c:38
#4 0x406ea7 in mysofa_open_default libmysofa-master/src/hrtf/easy.c:63
#5 0x406ea7 in mysofa_open libmysofa-master/src/hrtf/easy.c:86
#6 0x4022d4 in main libmysofa-master/test_libmysofa.c:116
#7 0x7fec7b5ed82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#8 0x402b48 in _start (libmysofa-master/test_libmysofa_asan.exe+0x402b48)
```

File triggering crash (unzip before test):
crash_002_changeAttribute.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 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-2020-36149 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