New issue

Jump to bottom

Heap buffer overflow in loudness #135

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

cve-reporting commented on Aug 26, 2020 • edited

Opening maliciously crafted file with mysofa_open leads to crash of the application.
Heap buffer overread by 126976 bytes in loudness() (libmysofa/src/hrtf/tools.c:179) cause segmentation fault.

Message from gdb:

```
Program received signal SIGSEGV, Segmentation fault.
0x000000000040fcdc in loudness (in=0x652000, size=240) at libmysofa-master/src/hrtf/tools.c:180
180 res += *in * *in;
```

AddressSanitizer report on crash:

```
ASAN:SIGSEGV
==5041==ERROR: AddressSanitizer: SEGV on unknown address 0x60200002d150 (pc 0x00000043180f bp 0x000000000ea6 sp 0x7fffe30a47f8 T0)
#0 0x43180e in loudness libmysofa-master/src/hrtf/tools.c:179
#1 0x43b6a2 in mysofa_loudness libmysofa-master/src/hrtf/loudness.c:49
#2 0x406e97 in mysofa_open_default libmysofa-master/src/hrtf/easy.c:56
#3 0x406e97 in mysofa_open libmysofa-master/src/hrtf/easy.c:86
#4 0x4022d4 in main libmysofa-master/test_libmysofa.c:116
#5 0x7f86208b682f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#6 0x402b48 in _start (libmysofa-master/test_libmysofa_asan.exe+0x402b48)
```

File triggering crash (unzip before test):
crash_000_loudness.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-2020-36150 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