New issue

Jump to bottom

Heap buffer overflow in mysofa_resampler_reset_mem #134

Closed **cve-reporting** opened this issue on Aug 25, 2020 · 3 comments

cve-reporting commented on Aug 25, 2020 • edited

Opening maliciously crafted file with mysofa_open leads to crash of the application.
Heap buffer overflow is caused by zeroing memory block of size (-1 casted to unsigned) in mysofa_resampler_reset_mem (speex_resampler.c:798).

AddressSanitizer report on crash:

```
==4759==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61600000fbfc at pc 0x7f396b3d3bec bp 0x7fff70a7c110 sp 0x7fff70a7b8b8
WRITE of size 17179869180 at 0x61600000fbfc thread T0
#0 0x7f396b3d3beb in __asan_memset (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8cbeb)
#1 0x4451fa in mysofa_resampler_reset_mem libmysofa-master/src/resampler/speex_resampler.c:791
#2 0x439f7c in mysofa_resample libmysofa-master/src/hrtf/resample.c:55
#3 0x406e39 in mysofa_open_default libmysofa-master/src/hrtf/easy.c:49
#4 0x406e39 in mysofa_open libmysofa-master/src/hrtf/easy.c:86
#5 0x4022d4 in main libmysofa-master/test_libmysofa.c:116
#6 0x7f396aa7a82f 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_008_mysofa_resampler_reset_mem.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 were not tested so far)

hoene commented on Nov 28, 2020 Owner

seams to be already fixed with one of the other commits

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-2020-36151 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