New issue

Jump to bottom

Double free vulnerability cause buffer overflow #319

Closed x00x00x00x00 opened this issue on Jun 6, 2021 · 1 comment

Labels bug

x00x00x00x00 commented on Jun 6, 2021

Hi Team,

Double-Free vulnerability cause buffer overflow is observed in miniaudio.h while fuzzing **MINIAUDIO (v0.10.35 and master branch)** using **ASAN** with **AFL FUZZER**

Steps to Reproduce -

cd examples

afl-gcc -fsanitize=address -fsanitize=leak -fsanitize=undefined simple_looping.c -o simple_looping -ldl -lm -lpthread

./simple_looping POC1

Download link to POC1

OUTPUT -

```
=================================================================
==2775==ERROR: AddressSanitizer: attempting double-free on 0x615000000080 in thread T0:
-0 0x7f68180667cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
-1 0x7f6817307042 in _IO_fclose (/lib/x86_64-linux-gnu/libc.so.6+0x85042)
-2 0x7f6818064908 in __interceptor_fclose (/lib/x86_64-linux-gnu/libasan.so.5+0x10b908)
-3 0x5649865b7e0b in ma_default_vfs_close__stdio ../miniaudio.h:44307
-4 0x5649865b7e0b in ma_default_vfs_close ../miniaudio.h:44491
-5 0x5649865b7e0b in ma_vfs_or_default_close ../miniaudio.h:44624
-6 0x5649865b7e0b in ma_vfs_or_default_close ../miniaudio.h:44619
-7 0x5649865b7e0b in ma_decoder_init_vfs ../miniaudio.h:47429
-8 0x564986018047 in ma_decoder_init_file ../miniaudio.h:47768
-9 0x564986018047 in main /home/zero/newfuz/audio/1/examples/simple_looping.c:43
-10 0x7f68172a90b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
-11 0x56498601889d in _start (/home/zero/newfuz/audio/1/examples/simple_looping+0x30c89d)

0x615000000080 is located 0 bytes inside of 472-byte region [0x615000000080,0x615000000258)
freed by thread T0 here:
-0 0x7f68180667cf in __interceptor_free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
-1 0x7f6817307042 in _IO_fclose (/lib/x86_64-linux-gnu/libc.so.6+0x85042)

previously allocated by thread T0 here:
-0 0x7f6818066bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
-1 0x7f6817307aad in _IO_fopen (/lib/x86_64-linux-gnu/libc.so.6+0x85aad)

SUMMARY: AddressSanitizer: double-free (/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf) in __interceptor_free
==2775==ABORTING
```

Request team to implement proper patch and validate

mackron added a commit that referenced this issue on Jun 11, 2021

`Fix a possible double file close when decoder initialization fails.` ··· `8234df8`

mackron commented on Jun 11, 2021 Owner

Thanks for the report. This should be fixed in the dev branch and will be released shortly. Feel free to reopen this issue if it's still not fixed properly.

mackron closed this as completed on Jun 11, 2021

mackron added the bug label on Jun 11, 2021

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants