SoX - Sound eXchange Bugs

Brought to you by: cbagwell, mansr, robs, uklauer

#360 [BUG] two bugs in sox

Status: open **Owner:** nobody **Labels:** None
Priority: 5
Updated: 2022-05-24 **Created:** 2022-05-24 **Creator:** Han Zheng **Private:** No

summary

Hello, I was testing my new fuzzer and found two bugs: a reachable assertion in rate_init, rate.c:303 and a float point exception in lsx_aiffstartwrite.

environment

sox latest commit 42b3557e13e0fe01a83465b672d89faddbe65f49,
clang 12.0.1,
Ubuntu 21.10

step to reproduce

compile sox with CC=clang, CFLAGS="-fsanitize=address -g"
run command `./sox --single-threaded @@ -t aiff /dev/null`

BUG1

```
sox: rate.c:303: void rate_init(rate_t *, rate_shared_t *, double, double, double, double, d
Aborted
```

BUG2

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3050061==ERROR: AddressSanitizer: FPE on unknown address 0x000000591211 (pc 0x00000059121
    #0 0x591211 in lsx_aiffstartwrite (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x591211)
    #1 0x83e26f in open_write (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x83e26f)
    #2 0x83b303 in sox_open_write (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x83b303)
    #3 0x8a4ae8 in open_output_file (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x8a4ae8)
    #4 0x8952e1 in process (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x8952e1)
    #5 0x887e23 in main (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x887e23)
    #6 0x7fac08e4afcf in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
    #7 0x7fac08e4b07c in __libc_start_main_impl ../csu/libc-start.c:409
    #8 0x408864 in _start (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x408864)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE (/home/kdsj/workspace/fuzz/sox-aiff/sox+0x591211) in lsx_aiff
==3050061==ABORTING
```

POC

as shown in attachment `poc.zip`

Credit

NCNIPC of China
Hexhive

1 Attachments

poc.zip

Discussion

Log in to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters
225 Broadway Suite 1600
San Diego, CA 92101
+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

Terms Privacy Opt Out Advertise