SoX - Sound eXchange Bugs

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

#349 div zero crash in wav.c

Status: open **Owner:** nobody **Labels:** bug (6)
Priority: 5
Updated: 2021-04-20 **Created:** 2021-04-20 **Creator:** treebacker **Private:** No

There is a `div zero` bug in wav.c:967, funcion `startread`.
With crafted wav file, it crashes.
Trigger command: ./src/.libs/sox bug1 -n noiseprof /dev/null

In AddressSanitizer:

```
ubuntu@VM-0-3-ubuntu:~/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/sox-code$ ./src/.libs/s
ASAN:DEADLYSIGNAL
=================================================================
==14604==ERROR: AddressSanitizer: FPE on unknown address 0x7eff2bdec8ec (pc 0x7eff2bdec8ec bp 0x7
    #0 0x7eff2bdec8eb in startread /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #1 0x7eff2bcfb460 in open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #2 0x7eff2bcfbcaa in sox_open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code
    #3 0x5622260ab58b in main /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/sox
    #4 0x7eff2b314bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #5 0x562226094339 in _start (/home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/so
==14604==ABORTING
```

In gdb:

```
gdb-peda$ r
Starting program: [redacted]/sox-code/src/.libs/sox [redacted]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGFPE, Arithmetic exception.
[----------------------------------registers-----------------------------------]
RAX: 0xe580
RBX: 0xe580
RCX: 0x1
RDX: 0x0
RSI: 0x0
RDI: 0x7ffff7dcefe0 --> 0x1
RBP: 0x0
RSP: 0x7fffffffe320 --> 0x0
RIP: 0x7ffff7b7d2f5 (<startread+7733>:  div    rsi)
R8 : 0xb40 ('@\x0b')
R9 : 0x2e ('.')
R10: 0x7ffff7fd0d00 (0x00007ffff7fd0d00)
R11: 0x246
R12: 0x61d528 --> 0x61db30 --> 0x0
R13: 0x6f99c0 --> 0x6faee0 ("out/uniq/bug1")
R14: 0x6faf00 --> 0x0
R15: 0x0
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x7ffff7b7d2ec <startread+7724>:     mov    esi,DWORD PTR [r13+0x2c]
   0x7ffff7b7d2f0 <startread+7728>:     xor    edx,edx
   0x7ffff7b7d2f2 <startread+7730>:     mov    rax,rbx
=> 0x7ffff7b7d2f5 <startread+7733>:     div    rsi
   0x7ffff7b7d2f8 <startread+7736>:     xor    edx,edx
   0x7ffff7b7d2fa <startread+7738>:     div    rcx
   0x7ffff7b7d2fd <startread+7741>:     mov    rbp,rax
   0x7ffff7b7d300 <startread+7744>:     mov    QWORD PTR [r14],rax
[-------------------------------------stack-------------------------------------]
0000| 0x7fffffffe320 --> 0x0
0008| 0x7fffffffe328 --> 0x1
0016| 0x7fffffffe330 --> 0x6faf00 --> 0x0
0024| 0x7fffffffe338 --> 0x40e5888000000001
0032| 0x7fffffffe340 --> 0x1cb0
0040| 0x7fffffffe348 --> 0x1cb000000000
0048| 0x7fffffffe350 --> 0x6f96f0 --> 0x0
0056| 0x7fffffffe358 --> 0x14110
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGFPE
0x00007ffff7b7d2f5 in startread (ft=0x6f99c0) at wav.c:967
967             wav->numSamples = div_bits(qwDataLength, ft->encoding.bits_per_sample)
gdb-peda$ bt
#0  0x00007ffff7b7d2f5 in startread (ft=0x6f99c0) at wav.c:967
#1  0x00007ffff7abaf49 in open_read (path=0x6f9680 "out/uniq/bug1", buffer=0x7ffff7bbae4b, buffer
#2  0x0000000000404c33 in main (argc=argc@entry=0x5, argv=<optimized out>, argv@entry=0x7fffffffe
#3  0x00007ffff710bbf7 in __libc_start_main (main=0x403100 <main>, argc=0x5, argv=0x7fffffffe898,
    at ../csu/libc-start.c:310
#4  0x000000000040303a in _start ()
```

The crafted file is attached.

1 Attachments

bug1

Discussion

Log in to post a comment.

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