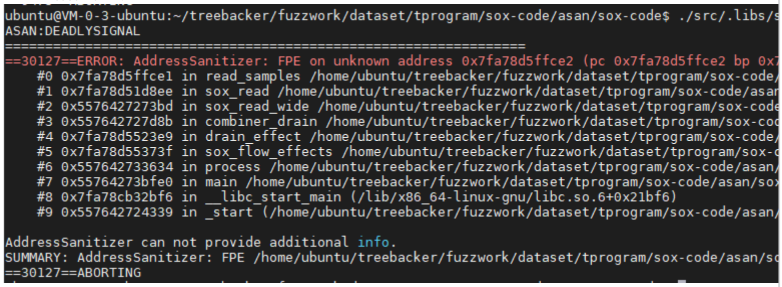
SoX - Sound eXchange Bugs

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

#351 div zero in voc.c

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

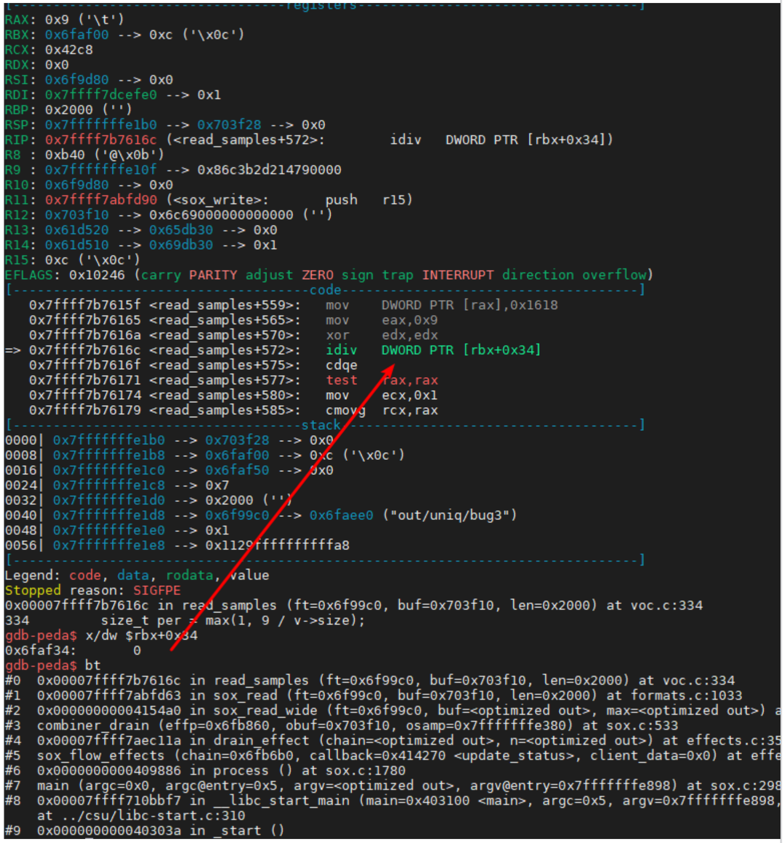
There is a `div zero` in voc.c:334, functon `read_samples`.
Which crashes.
The trigger command: ./src/.libs/sox bug3 -n noiseprof /dev/null
In AddressSanitizer:



```
ubuntu@VM-0-3-ubuntu:~/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/sox-code$ ./src/.libs/s
ASAN:DEADLYSIGNAL
=================================================================
==30127==ERROR: AddressSanitizer: FPE on unknown address 0x7fa78d5ffce2 (pc 0x7fa78d5ffce2 bp 0x7
    #0 0x7fa78d5ffce1 in read_samples /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/
    #1 0x7fa78d51d8ee in sox_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan
    #2 0x5576427273bd in sox_read_wide /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code
    #3 0x557642727d8b in combiner_drain /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-coc
    #4 0x7fa78d5523e9 in drain_effect /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/
    #5 0x7fa78d55373f in sox_flow_effects /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-c
    #6 0x557642733634 in process /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/
    #7 0x55764273bfe0 in main /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/sox
    #8 0x7fa78cb32bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #9 0x557642724339 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/sc
==30127==ABORTING
```

In gdb:



```
[----------------------------------registers-----------------------------------]
RAX: 0x9 ('\t')
RBX: 0x6faf00 --> 0xc ('\x0c')
RCX: 0x42c8
RDX: 0x0
RSI: 0x6f9d80 --> 0x0
RDI: 0x7ffff7dcefe0 --> 0x1
RBP: 0x2000 ('')
RSP: 0x7fffffffe1b0 --> 0x703f28 --> 0x0
RIP: 0x7ffff7b7616c (<read_samples+572>:        idiv   DWORD PTR [rbx+0x34])
R8 : 0xb40 ('@\x0b')
R9 : 0x7fffffffe10f --> 0x86c3b2d214790000
R10: 0x6f9d80 --> 0x0
R11: 0x7ffff7abfd90 (<sox_write>:       push   r15)
R12: 0x703f10 --> 0x6c69000000000000 ('')
R13: 0x61d520 --> 0x65db30 --> 0x0
R14: 0x61d510 --> 0x69db30 --> 0x1
R15: 0xc ('\x0c')
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x7ffff7b7615f <read_samples+559>:   mov    DWORD PTR [rax],0x1618
   0x7ffff7b76165 <read_samples+565>:   mov    eax,0x9
   0x7ffff7b7616a <read_samples+570>:   xor    edx,edx
=> 0x7ffff7b7616c <read_samples+572>:   idiv   DWORD PTR [rbx+0x34]
   0x7ffff7b7616f <read_samples+575>:   cdqe
   0x7ffff7b76171 <read_samples+577>:   test   rax,rax
   0x7ffff7b76174 <read_samples+580>:   mov    ecx,0x1
   0x7ffff7b76179 <read_samples+585>:   cmovg  rcx,rax
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffe1b0 --> 0x703f28 --> 0x0
0008| 0x7fffffffe1b8 --> 0x6faf00 --> 0xc ('\x0c')
0016| 0x7fffffffe1c0 --> 0x6faf50 --> 0x0
0024| 0x7fffffffe1c8 --> 0x7
0032| 0x7fffffffe1d0 --> 0x2000 ('')
0040| 0x7fffffffe1d8 --> 0x6f99c0 --> 0x6faee0 ("out/uniq/bug3")
0048| 0x7fffffffe1e0 --> 0x1
0056| 0x7fffffffe1e8 --> 0x1129ffffffffffa8
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGFPE
0x00007ffff7b7616c in read_samples (ft=0x6f99c0, buf=0x703f10, len=0x2000) at voc.c:334
334         size_t per = max(1, 9 / v->size);
gdb-peda$ x/dw $rbx+0x34
0x6faf34:       0
gdb-peda$ bt
#0  0x00007ffff7b7616c in read_samples (ft=0x6f99c0, buf=0x703f10, len=0x2000) at voc.c:334
#1  0x00007ffff7abfd63 in sox_read (ft=0x6f99c0, buf=0x703f10, len=0x2000) at formats.c:1033
#2  0x00000000004154a0 in sox_read_wide (ft=0x6f99c0, buf=<optimized out>, max=<optimized out>) a
#3  combiner_drain (effp=0x6fb860, obuf=0x703f10, osamp=0x7fffffffe380) at sox.c:533
#4  0x00007ffff7aec11a in drain_effect (chain=<optimized out>, n=<optimized out>) at effects.c:35
#5  sox_flow_effects (chain=0x6fb6b0, callback=0x414270 <update_status>, client_data=0x0) at effe
#6  0x0000000000409886 in process () at sox.c:1780
#7  main (argc=0x0, argc@entry=0x5, argv=<optimized out>, argv@entry=0x7fffffffe898) at sox.c:298
#8  0x00007ffff710bbf7 in __libc_start_main (main=0x403100 <main>, argc=0x5, argv=0x7fffffffe898,
    at ../csu/libc-start.c:310
#9  0x000000000040303a in _start ()
```

The crafted file is attached.

1 Attachments

bug3

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