SoX - Sound eXchange Bugs

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

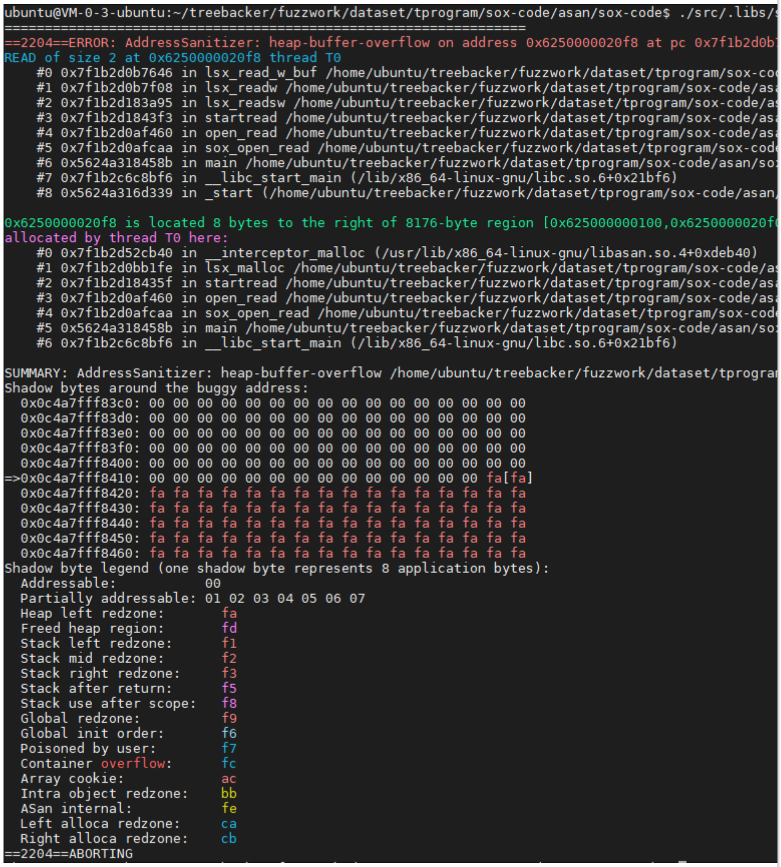
#352 heap-overflow in formats_i.c

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

There is a heap overflow in formats_i.c:376, function `lsx_read_w_buf`.

Trigger command:

In In AddressSanitizer:

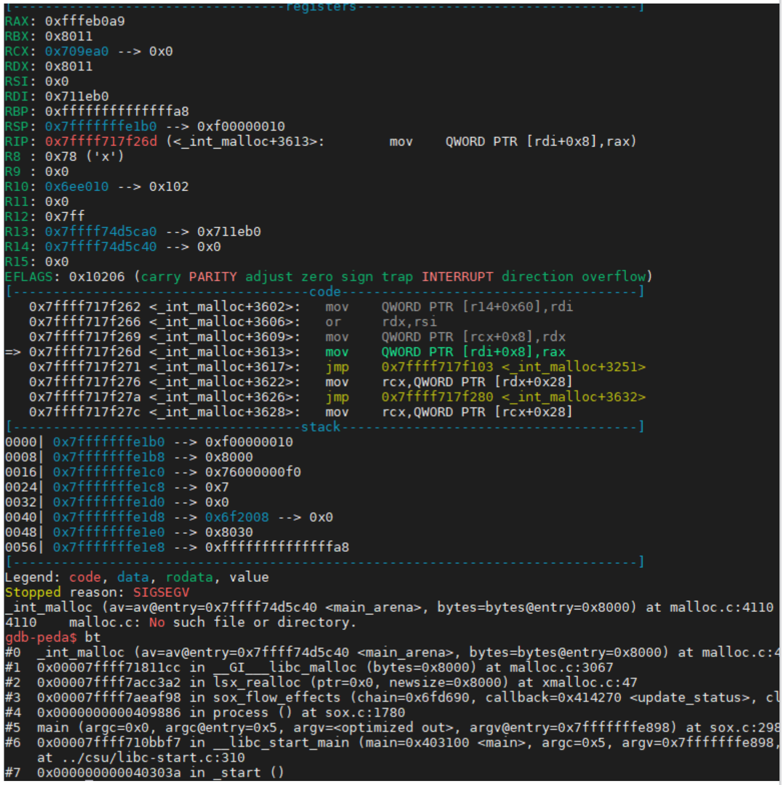


```
ubuntu@VM-0-3-ubuntu:~/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/sox-code$ ./src/.libs/s
=================================================================
==2204==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6250000020f8 at pc 0x7f1b2d0b7
READ of size 2 at 0x6250000020f8 thread T0
    #0 0x7f1b2d0b7646 in lsx_read_w_buf /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-coc
    #1 0x7f1b2d0b7f08 in lsx_readw /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #2 0x7f1b2d183a95 in lsx_readsw /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/as
    #3 0x7f1b2d1843f3 in startread /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #4 0x7f1b2d0af460 in open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #5 0x7f1b2d0afcaa in sox_open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code
    #6 0x5624a318458b in main /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/so
    #7 0x7f1b2c6c8bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #8 0x5624a316d339 in _start (/home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/

0x6250000020f8 is located 8 bytes to the right of 8176-byte region [0x625000000100,0x6250000020f
allocated by thread T0 here:
    #0 0x7f1b2d52cb40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f1b2d0bb1fe in lsx_malloc /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/as
    #2 0x7f1b2d18435f in startread /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #3 0x7f1b2d0af460 in open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asa
    #4 0x7f1b2d0afcaa in sox_open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code
    #5 0x5624a318458b in main /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/so
    #6 0x7f1b2c6c8bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/ubuntu/treebacker/fuzzwork/dataset/tprogra
Shadow bytes around the buggy address:
  0x0c4a7fff83c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff83d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff83e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff83f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fff8400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c4a7fff8410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa[fa]
  0x0c4a7fff8420: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff8430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff8440: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff8450: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff8460: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==2204==ABORTING
```

In gdb:



```
[----------------------------------registers-----------------------------------]
RAX: 0xfffeb0a9
RBX: 0x8011
RCX: 0x709ea0 --> 0x0
RDX: 0x8011
RSI: 0x0
RDI: 0x711eb0
RBP: 0xffffffffffffffa8
RSP: 0x7fffffffe1b0 --> 0xf00000010
RIP: 0x7ffff717f26d (<_int_malloc+3613>:        mov    QWORD PTR [rdi+0x8],rax)
R8 : 0x78 ('x')
R9 : 0x0
R10: 0x6ee010 --> 0x102
R11: 0x0
R12: 0x7ff
R13: 0x7ffff74d5ca0 --> 0x711eb0
R14: 0x7ffff74d5c40 --> 0x0
R15: 0x0
EFLAGS: 0x10206 (carry PARITY adjust zero sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x7ffff717f262 <_int_malloc+3602>:   mov    QWORD PTR [r14+0x60],rdi
   0x7ffff717f266 <_int_malloc+3606>:   or     rdx,rsi
   0x7ffff717f269 <_int_malloc+3609>:   mov    QWORD PTR [rcx+0x8],rdx
=> 0x7ffff717f26d <_int_malloc+3613>:   mov    QWORD PTR [rdi+0x8],rax
   0x7ffff717f271 <_int_malloc+3617>:   jmp    0x7ffff717f103 <_int_malloc+3251>
   0x7ffff717f276 <_int_malloc+3622>:   mov    rcx,QWORD PTR [rdx+0x28]
   0x7ffff717f27a <_int_malloc+3626>:   jmp    0x7ffff717f280 <_int_malloc+3632>
   0x7ffff717f27c <_int_malloc+3628>:   mov    rcx,QWORD PTR [rcx+0x28]
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffe1b0 --> 0xf00000010
0008| 0x7fffffffe1b8 --> 0x8000
0016| 0x7fffffffe1c0 --> 0x76000000f0
0024| 0x7fffffffe1c8 --> 0x7
0032| 0x7fffffffe1d0 --> 0x0
0040| 0x7fffffffe1d8 --> 0x6f2008 --> 0x0
0048| 0x7fffffffe1e0 --> 0x8030
0056| 0x7fffffffe1e8 --> 0xffffffffffffffa8
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
_int_malloc (av=av@entry=0x7ffff74d5c40 <main_arena>, bytes=bytes@entry=0x8000) at malloc.c:4110
4110    malloc.c: No such file or directory.
gdb-peda$ bt
#0  _int_malloc (av=av@entry=0x7ffff74d5c40 <main_arena>, bytes=bytes@entry=0x8000) at malloc.c:4
#1  0x00007ffff71811cc in __GI___libc_malloc (bytes=0x8000) at malloc.c:3067
#2  0x00007ffff7acc3a2 in lsx_realloc (ptr=0x0, newsize=0x8000) at xmalloc.c:47
#3  0x00007ffff7aeaf98 in sox_flow_effects (chain=0x6fd690, callback=0x414270 <update_status>, cl
#4  0x0000000000409886 in process () at sox.c:1780
#5  main (argc=0x0, argc@entry=0x5, argv=<optimized out>, argv@entry=0x7fffffffe898) at sox.c:298
#6  0x00007ffff710bbf7 in __libc_start_main (main=0x403100 <main>, argc=0x5, argv=0x7fffffffe898,
    at ../csu/libc-start.c:310
#7  0x000000000040303a in _start ()
```

The crafted file is attached.

1 Attachments

bug4

Discussion

Log in to post a comment.