SoX - Sound eXchange Bugs

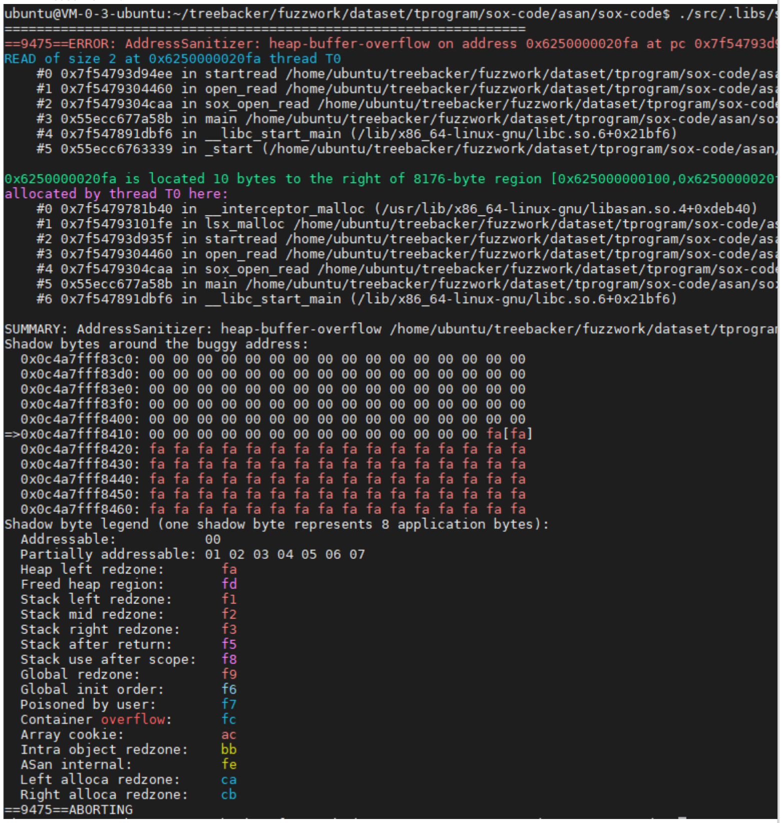
Brought to you by: cbagwell, mansr, robs, uklauer

#350 Heap overflow in hcom.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 hcom.c:161. Function `startread`.
With crafted hcomn file, the vuln is exploitable.
Trigger command: ./src/.libs/sox bug2 -n noiseprof /dev/null

In AddressSanitizer:

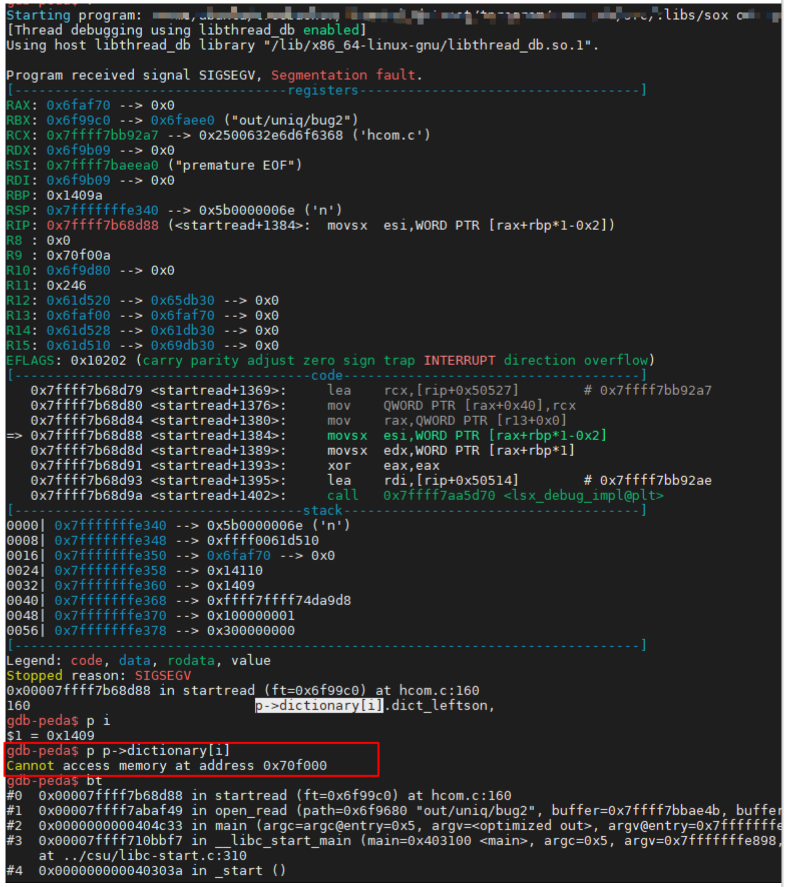


```
ubuntu@VM-0-3-ubuntu:~/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/sox-code$ ./src/.libs/
=================================================================
==9475==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6250000020fa at pc 0x7f54793d
READ of size 2 at 0x6250000020fa thread T0
    #0 0x7f54793d94ee in startread /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/as
    #1 0x7f5479304460 in open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/as
    #2 0x7f5479304caa in sox_open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-cod
    #3 0x55ecc677a58b in main /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/so
    #4 0x7f547891dbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #5 0x55ecc6763339 in _start (/home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan

0x6250000020fa is located 10 bytes to the right of 8176-byte region [0x625000000100,0x6250000020
allocated by thread T0 here:
    #0 0x7f5479781b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f54793101fe in lsx_malloc /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/a
    #2 0x7f54793d935f in startread /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/as
    #3 0x7f5479304460 in open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/as
    #4 0x7f5479304caa in sox_open_read /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-cod
    #5 0x55ecc677a58b in main /home/ubuntu/treebacker/fuzzwork/dataset/tprogram/sox-code/asan/so
    #6 0x7f547891dbf6 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
==9475==ABORTING
```

In gdb:



```
Starting program: [redacted].libs/sox c[redacted]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
RAX: 0x6faf70 --> 0x0
RBX: 0x6f99c0 --> 0x6faee0 ("out/uniq/bug2")
RCX: 0x7ffff7bb92a7 --> 0x2500632e6d6f6368 ('hcom.c')
RDX: 0x6f9b09 --> 0x0
RSI: 0x7ffff7baeea0 ("premature EOF")
RDI: 0x6f9b09 --> 0x0
RBP: 0x1409a
RSP: 0x7fffffffe340 --> 0x5b0000006e ('n')
RIP: 0x7ffff7b68d88 (<startread+1384>:  movsx  esi,WORD PTR [rax+rbp*1-0x2])
R8 : 0x0
R9 : 0x70f00a
R10: 0x6f9d80 --> 0x0
R11: 0x246
R12: 0x61d520 --> 0x65db30 --> 0x0
R13: 0x6faf00 --> 0x6faf70 --> 0x0
R14: 0x61d528 --> 0x61db30 --> 0x0
R15: 0x61d510 --> 0x69db30 --> 0x0
EFLAGS: 0x10202 (carry parity adjust zero sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x7ffff7b68d79 <startread+1369>:     lea    rcx,[rip+0x50527]        # 0x7ffff7bb92a7
   0x7ffff7b68d80 <startread+1376>:     mov    QWORD PTR [rax+0x40],rcx
   0x7ffff7b68d84 <startread+1380>:     mov    rax,QWORD PTR [r13+0x0]
=> 0x7ffff7b68d88 <startread+1384>:     movsx  esi,WORD PTR [rax+rbp*1-0x2]
   0x7ffff7b68d8d <startread+1389>:     movsx  edx,WORD PTR [rax+rbp*1]
   0x7ffff7b68d91 <startread+1393>:     xor    eax,eax
   0x7ffff7b68d93 <startread+1395>:     lea    rdi,[rip+0x50514]        # 0x7ffff7bb92ae
   0x7ffff7b68d9a <startread+1402>:     call   0x7ffff7aa5d70 <lsx_debug_impl@plt>
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffe340 --> 0x5b0000006e ('n')
0008| 0x7fffffffe348 --> 0xffff0061d510
0016| 0x7fffffffe350 --> 0x6faf70 --> 0x0
0024| 0x7fffffffe358 --> 0x14110
0032| 0x7fffffffe360 --> 0x1409
0040| 0x7fffffffe368 --> 0xffff7ffff74da9d8
0048| 0x7fffffffe370 --> 0x100000001
0056| 0x7fffffffe378 --> 0x300000000
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x00007ffff7b68d88 in startread (ft=0x6f99c0) at hcom.c:160
160                             p->dictionary[i].dict_leftson,
gdb-peda$ p i
$1 = 0x1409
gdb-peda$ p p->dictionary[i]
Cannot access memory at address 0x70f000
gdb-peda$ bt
#0  0x00007ffff7b68d88 in startread (ft=0x6f99c0) at hcom.c:160
#1  0x00007ffff7abaf49 in open_read (path=0x6f9680 "out/uniq/bug2", 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

bug2

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