New issue

Jump to bottom

A heap-buffer-overflow in wav_file.cpp:160:40 #23

Open seviezhou opened this issue on Aug 13, 2020 · 0 comments

seviezhou commented on Aug 13, 2020 • edited

System info

Ubuntu x86_64, clang 6.0, sela (latest master ca09cb)

Configure

cmake .. -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address" -DCMAKE_MODULE_LINKER_FLAGS="-fsanitize=address"

Command line

./build/sela -e @@ /dev/null

AddressSanitizer output

```
=================================================================
==65004==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000008d0 at pc 0x00000055d64b bp 0x7ffc37ec4b00 sp 0x7ffc37ec4af8
READ of size 1 at 0x6160000008d0 thread T0
    #0 0x55d64a in signed char* std::__copy_move<false, false, std::random_access_iterator_tag>::__copy_m<char*, signed char*>(char*, char*, signed char*) /usr/lib/gcc/x86_64-
linux-gnu/8/../../../../include/c++/8/bits/stl_algobase.h:324:20
    #1 0x55d64a in signed char* std::__copy_move_a<false, char*, signed char*>(char*, char*, signed char*) /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/stl_algobase.h:385
    #2 0x55d64a in signed char* std::__copy_move_a2<false, __gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, signed char*>
(__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, __gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, signed char*)
/usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_algobase.h:422
    #3 0x55d42b in void std::vector<signed char, std::allocator<signed char> >::_M_range_initialize<__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > > >
(__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, __gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >,
std::forward_iterator_tag) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_algobase.h:454:15
    #4 0x557b9b in void std::vector<signed char, std::allocator<signed char> >::_M_initialize_dispatch<__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> >
> >(__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, __gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >,
std::__false_type) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_vector.h:1437:4
    #5 0x557b9b in std::vector<signed char, std::allocator<signed char> >::vector<__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, void>
(__gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >, __gnu_cxx::__normal_iterator<char*, std::vector<char, std::allocator<char> > >,
std::allocator<signed char> const&) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_vector.h:546
    #6 0x55156b in file::WavFile::readFromFile(std::basic_ifstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/file/wav_file.cpp:160:40
    #7 0x5655b3 in sela::Encoder::readFrames() /home/seviezhou/sela/src/sela/encoder.cpp:37:13
    #8 0x5655b3 in sela::Encoder::process() /home/seviezhou/sela/src/sela/encoder.cpp:97
    #9 0x51d568 in encodeFile(std::basic_ifstream<char, std::char_traits<char> >&, std::basic_ofstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/main.cpp:32:39
    #10 0x51ef56 in main /home/seviezhou/sela/src/main.cpp:75:17
    #11 0x7f16fe66183f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #12 0x41c5e8 in _start (/home/seviezhou/sela/build/sela+0x41c5e8)

0x6160000008d0 is located 0 bytes to the right of 592-byte region [0x616000000680,0x6160000008d0)
allocated by thread T0 here:
    #0 0x518278 in operator new(unsigned long) /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_new_delete.cc:92
    #1 0x54c83a in __gnu_cxx::new_allocator<char>::allocate(unsigned long, void const*) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/ext/new_allocator.h:111:27
    #2 0x54c83a in std::allocator_traits<std::allocator<char> >::allocate(std::allocator<char>&, unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/alloc_traits.h:436
    #3 0x54c83a in std::_Vector_base<char, std::allocator<char> >::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_vector.h:296
    #4 0x54c83a in std::vector<char, std::allocator<char> >::_M_default_append(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/vector.tcc:604

SUMMARY: AddressSanitizer: heap-buffer-overflow /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_algobase.h:324:20 in signed char* std::__copy_move<false, false,
std::random_access_iterator_tag>::__copy_m<char*, signed char*>(char*, char*, signed char*)
Shadow bytes around the buggy address:
  0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff80e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff80f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff8100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2c7fff8110: 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa fa fa
  0x0c2c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8160: 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
==65004==ABORTING
```

POC

heap-overflow-readFromFile-wav_file-160.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant