New issue

Jump to bottom

A heap-buffer-overflow in wav_file.cpp:262:32 #25

⊙ Open **seviezhou** opened this issue on Aug 14, 2020 · 0 comments

seviezhou commented on Aug 14, 2020

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 -d @@ /dev/null

AddressSanitizer output

```
=================================================================
==42335==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x625001498100 at pc 0x000000445201 bp 0x7ffc5546e9f0 sp 0x7ffc5546e1a0
READ of size 18 at 0x625001498100 thread T0
    #0 0x445200 in __interceptor_memcpy.part.37 /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:779
    #1 0x7fe75bdf4387 in std::basic_streambuf<char, std::char_traits<char> >::xsputn(char const*, long) (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0x13d387)
    #2 0x7fe75bde3262 in std::ostream::write(char const*, long) (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0x12c262)
    #3 0x557736 in file::WavFile::writeToFile(std::basic_ofstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/file/wav_file.cpp:262:32
    #4 0x51dc13 in decodeFile(std::basic_ifstream<char, std::char_traits<char> >&, std::basic_ofstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/main.cpp:40:13
    #5 0x51f553 in main /home/seviezhou/sela/src/main.cpp:85:17
    #6 0x7fe75adc383f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #7 0x41c5e8 in _start (/home/seviezhou/sela/build/sela+0x41c5e8)

0x625001498100 is located 0 bytes to the right of 8192-byte region [0x625001496100,0x625001498100)
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 0x525759 in __gnu_cxx::new_allocator<int>::allocate(unsigned long, void const*) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/ext/new_allocator.h:111:27
    #2 0x525759 in std::allocator_traits<std::allocator<int> >::allocate(std::allocator<int>&, unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/alloc_traits.h:436
    #3 0x525759 in std::_Vector_base<int, std::allocator<int> >::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_vector.h:296
    #4 0x525759 in std::_Vector_base<int, std::allocator<int> >::_M_create_storage(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_vector.h:311
    #5 0x525759 in std::_Vector_base<int, std::allocator<int> >::_Vector_base(unsigned long, std::allocator<int> const&) /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/stl_vector.h:260
    #6 0x5576d6 in file::WavFile::writeToFile(std::basic_ofstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/file/wav_file.cpp:261:51
    #7 0x51dc13 in decodeFile(std::basic_ifstream<char, std::char_traits<char> >&, std::basic_ofstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/main.cpp:40:13
    #8 0x51f553 in main /home/seviezhou/sela/src/main.cpp:85:17
    #9 0x7fe75adc383f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:779 in
__interceptor_memcpy.part.37
Shadow bytes around the buggy address:
  0x0c4a8028afd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a8028afe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a8028aff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a8028b000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a8028b010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c4a8028b020:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8028b030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8028b040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8028b050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8028b060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a8028b070: 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
==42335==ABORTING
```

POC

heap-overflow-writeToFile-wav_file-262.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant