New issue

Jump to bottom

A heap-buffer-overflow in rice_decoder.cpp:39 #29

⊙ 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

```
=================================================================
==28346==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001058 at pc 0x00000053ad8d bp 0x7f61d7aaf0b0 sp 0x7f61d7aaf0a8
READ of size 8 at 0x602000001058 thread T80
    #0 0x53ad8c in std::_Bit_reference::operator bool() const /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_bvector.h:83:17
    #1 0x53ad8c in rice::RiceDecoder::generateDecodedUnsignedInts() /home/seviezhou/sela/src/rice/rice_decoder.cpp:39
    #2 0x53a05b in rice::RiceDecoder::process() /home/seviezhou/sela/src/rice/rice_decoder.cpp:58:5
    #3 0x541287 in frame::FrameDecoder::process() /home/seviezhou/sela/src/frame/frame_decoder.cpp:28:93
    #4 0x56e3fe in sela::LoopThrough::process(std::vector<data::WavFrame, std::allocator<data::WavFrame> >&) /home/seviezhou/sela/src/sela/decoder.cpp:30:47
    #5 0x7f6202d78b0f  (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0xd0b0f)
    #6 0x7f62027896b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
    #7 0x7f6201e9b4dc in clone /build/glibc-e6zv40/glibc-2.23/misc/../sysdeps/unix/sysv/linux/x86_64/clone.S:109

0x602000001058 is located 0 bytes to the right of 8-byte region [0x602000001050,0x602000001058)
allocated by thread T80 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 0x534dcd in __gnu_cxx::new_allocator<unsigned long>::allocate(unsigned long, void const*) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/ext/new_allocator.h:111:27
    #2 0x534dcd in std::allocator_traits<std::allocator<unsigned long> >::allocate(std::allocator<unsigned long>&, unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/alloc_traits.h:436
    #3 0x534dcd in std::_Bvector_base<std::allocator<bool> >::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_bvector.h:530
    #4 0x534dcd in std::vector<bool, std::allocator<bool> >::_M_reallocate(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/vector.tcc:764
    #5 0x534560 in std::vector<bool, std::allocator<bool> >::reserve(unsigned long) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_bvector.h:921:4

Thread T80 created by T0 here:
    #0 0x434b8d in pthread_create /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_interceptors.cc:204
    #1 0x7f6202d78da4 in std::thread::_M_start_thread(std::unique_ptr<std::thread::_State, std::default_delete<std::thread::_State> >, void (*)()) (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0xd0da4)
    #2 0x56c1ea in sela::Decoder::processFrames(std::vector<data::WavFrame, std::allocator<data::WavFrame> >&) /home/seviezhou/sela/src/sela/decoder.cpp:68:34
    #3 0x56d73b in sela::Decoder::process() /home/seviezhou/sela/src/sela/decoder.cpp:98:5
    #4 0x51dbe8 in decodeFile(std::basic_ifstream<char, std::char_traits<char> >&, std::basic_ofstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/main.cpp:39:37
    #5 0x51f553 in main /home/seviezhou/sela/src/main.cpp:85:17
    #6 0x7f6201db483f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291

SUMMARY: AddressSanitizer: heap-buffer-overflow /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_bvector.h:83:17 in std::_Bit_reference::operator bool() const
Shadow bytes around the buggy address:
  0x0c047fff81b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c047fff8200: fa fa 04 fa fa fa 04 fa fa fa 00[fa]fa fa 00 fa
  0x0c047fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8230: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8250: 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
==28346==ABORTING
```

POC

heap-overflow-generateDecodedUnsignedInts-rice_decoder-39.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant