

New issue

Jump to bottom

# A heap-buffer-overflow in sela\_file.cpp:78:67 #26

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

```
=====
==36806==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62a00005775 at pc 0x00000548d25 bp 0x7ffef4e9b430 sp 0x7ffef4e9b428
READ of size 1 at 0x62a00005775 thread T0
#0 0x548d24 in file::SelaFile::readFromFile(std::basic_ifstream<char, std::char_traits<char> >&) /home/seviezhou/sela/src/file/sela_file.cpp:78:67
#1 0x56d713 in sela::Decoder::readFrames() /home/seviezhou/sela/src/sela/decoder.cpp:38:14
#2 0x56d713 in sela::Decoder::process() /home/seviezhou/sela/src/sela/decoder.cpp:97
#3 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
#4 0x51f553 in main /home/seviezhou/sela/src/main.cpp:85:17
#5 0x7fa6b3dd783f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#6 0x41c5e8 in _start (/home/seviezhou/sela/build/sela+0x41c5e8)

0x62a00005775 is located 2 bytes to the right of 21875-byte region [0x62a00000200,0x62a00005773)
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 /home/seviezhou/sela/src/file/sela_file.cpp:78:67 in file::SelaFile::readFromFile(std::basic_ifstream<char, std::char_traits<char> >&)
Shadow bytes around the buggy address:
 0x0c547fff8a90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c547fff8aa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c547fff8ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c547fff8ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c547fff8ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c547fff8ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[03]fa
0x0c547fff8af0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c547fff8b00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c547fff8b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c547fff8b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c547fff8b30: 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
==36806==ABORTING
```

## POC

[heap-overflow-readFromFile-sela\\_file-78.zip](#)

Assignees  
No one assigned

Labels  
None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

