

New issue

Jump to bottom

Segmentation fault in wav_file.cpp:13:46 #27

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

```
AddressSanitizer:DEADLYSIGNAL
=====
==74467==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x00000054f6ca bp 0x7ffd122617f0 sp 0x7ffd122616a0 T0)
==74467==The signal is caused by a READ memory access.
==74467==Hint: address points to the zero page.
#0 0x54f6c9 in file::WavFile::WavFile(unsigned int, unsigned short, unsigned short, std::vector<data::WavFrame, std::allocator<data::WavFrame> >&&)
/home/seviezhou/sela/src/file/wav_file.cpp:13:46
#1 0x56d7da in sela::Decoder::process() /home/seviezhou/sela/src/sela/decoder.cpp:99:12
#2 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
#3 0x51f553 in main /home/seviezhou/sela/src/main.cpp:85:17
#4 0x7fb55432f83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#5 0x41c5e8 in _start (/home/seviezhou/sela/build/sela+0x41c5e8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/sela/src/file/wav_file.cpp:13:46 in file::WavFile::WavFile(unsigned int, unsigned short, unsigned short, std::vector<data::WavFrame, std::allocator<data::WavFrame> >&&)
==74467==ABORTING
```

POC

SEGV-WavFile-wav_file-13.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

