New issue

Jump to bottom

Segmentation fault in frame_decoder.cpp:65:35 #28

○ 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
=================================================================
==41926==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005422ce bp 0x7fc345bafcb0 sp 0x7fc345baf2c0 T80)
==41926==The signal is caused by a READ memory access.
==41926==Hint: address points to the zero page.
    #0 0x5422cd in frame::FrameDecoder::process() /home/seviezhou/sela/src/frame/frame_decoder.cpp:65:35
    #1 0x56e3fe in sela::LoopThrough::process(std::vector<data::WavFrame, std::allocator<data::WavFrame> >&) /home/seviezhou/sela/src/sela/decoder.cpp:30:47
    #2 0x7fc370e9bb0f  (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0xd0b0f)
    #3 0x7fc3708ac6b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
    #4 0x7fc36ffbe4dc in clone /build/glibc-e6zv40/glibc-2.23/misc/../sysdeps/unix/sysv/linux/x86_64/clone.S:109

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/sela/src/frame/frame_decoder.cpp:65:35 in frame::FrameDecoder::process()
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 0x7fc370e9bda4 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 0x7fc36fed783f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291

==41926==ABORTING
```

POC

SEGV-process-frame_decoder-65.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant