New issue

Jump to bottom

A Segmentation fault in nalutil.cpp:49:10 #85

Closed seviezhou opened this issue on Aug 4, 2020 · 1 comment

seviezhou commented on Aug 4, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), heif (latest master 2fc78e)

Configure

cmake ../srcs -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address"

Command line

modify example.cpp, use example7() to receive filename from commandline.

./build/bin/example @@

Output

```
Segmentation fault
```

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==63742==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005aebf2 bp 0x00000017e040 sp 0x7ffe4944ccd0 T0)
==63742==The signal is caused by a READ memory access.
==63742==Hint: address points to the zero page.
    #0 0x5aebf1 in
_ZNSt16allocator_traitsI9AllocatorIhEE12_S_constructIhJRKhEEENSt9enable_ifIXsr6__and_ISt6__and_IJSt6__not_INS2_18__construct_helperIT_JDpT0_EE4typeEESt16is_constructibleISA_JSC_EEEEEE
/usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/alloc_traits.h:250:26
    #1 0x5aebf1 in _ZNSt16allocator_traitsI9AllocatorIhEE9constructIhJRKhEEEDTcl12_S_constructfp_fp0_spcl5r3stdE7forwardIT0_Efp1_EEERS1_PT_DpOS6_ /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/alloc_traits.h:344
    #2 0x5aebf1 in unsigned char* std::__uninitialized_copy_a<__gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >, unsigned
char*, Allocator<unsigned char> >(__gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >, __gnu_cxx::__normal_iterator<unsigned
char const*, std::vector<unsigned char, Allocator<unsigned char> > >, unsigned char*, Allocator<unsigned char>&) /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/stl_uninitialized.h:275
    #3 0x6ed80a in void std::vector<unsigned char, Allocator<unsigned char> >::_M_range_insert<__gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char,
Allocator<unsigned char> > > >(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, Allocator<unsigned char> > >, __gnu_cxx::__normal_iterator<unsigned char
const*, std::vector<unsigned char, Allocator<unsigned char> > >, __gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >,
std::forward_iterator_tag) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/vector.tcc:729:11
    #4 0x6ec4bb in void std::vector<unsigned char, Allocator<unsigned char> >::_M_insert_dispatch<__gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char,
Allocator<unsigned char> > > >(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, Allocator<unsigned char> > >, __gnu_cxx::__normal_iterator<unsigned char
const*, std::vector<unsigned char, Allocator<unsigned char> > >, __gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >,
std::__false_type) /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/stl_vector.h:1549:4
    #5 0x6ec4bb in __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, Allocator<unsigned char> > > std::vector<unsigned char, Allocator<unsigned char>
>::insert<__gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >, void>(__gnu_cxx::__normal_iterator<unsigned char const*,
std::vector<unsigned char, Allocator<unsigned char> > >, __gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >,
__gnu_cxx::__normal_iterator<unsigned char const*, std::vector<unsigned char, Allocator<unsigned char> > >) /usr/lib/gcc/x86_64-linux-
gnu/8/../../../../include/c++/8/bits/stl_vector.h:1270
    #6 0x82d4ee in convertByteStreamToRBSP(std::vector<unsigned char, Allocator<unsigned char> > const&) /home/seviezhou/heif/srcs/common/nalutil.cpp:49:10
    #7 0x81b114 in HevcDecoderConfigurationRecord::makeConfigFromSPS(std::vector<unsigned char, Allocator<unsigned char> > const&)
/home/seviezhou/heif/srcs/common/hevcdecoderconfigrecord.cpp:52:27
    #8 0x88172d in HEIF::(anonymous namespace)::createHevcDecoderConfigurationRecord(HEIF::Array<HEIF::DecoderSpecificInfo> const&, HevcDecoderConfigurationRecord&)
/home/seviezhou/heif/srcs/writer/writermetaimpl.cpp:112:34
    #9 0x88172d in HEIF::WriterImpl::getConfigIndex(HEIF::DecoderConfigId, unsigned short&) /home/seviezhou/heif/srcs/writer/writermetaimpl.cpp:1191
    #10 0x87e1bf in HEIF::WriterImpl::addImage(HEIF::MediaDataId const&, HEIF::ImageId&) /home/seviezhou/heif/srcs/writer/writermetaimpl.cpp:199:31
    #11 0x52072f in main /home/seviezhou/heif/srcs/examples/example.cpp:104:29
    #12 0x7f7cca1e283f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #13 0x41f0b8 in _start (/home/seviezhou/heif/build/bin/example+0x41f0b8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /usr/lib/gcc/x86_64-linux-gnu/8/../../../../include/c++/8/bits/alloc_traits.h:250:26 in
_ZNSt16allocator_traitsI9AllocatorIhEE12_S_constructIhJRKhEEENSt9enable_ifIXsr6__and_ISt6__and_IJSt6__not_INS2_18__construct_helperIT_JDpT0_EE4typeEESt16is_constructibleISA_JSC_EEEEEE
==63742==ABORTING
```

POC

SEGV-convertByteStreamToRBSP-nalutil-49.zip

lassehe commented on Aug 12, 2020 Collaborator

Thank you for reporting this. The issue was fixed in commit b26a70.

 **lassehe** closed this as completed on Aug 12, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants