Heap buffer overflow #68

Open Cvjark opened this issue on Jul 15 · 0 comments

Cvjark commented on Jul 15

Hi, by testing this repo, i found something unusual.

crash sample

id0_heap_buffer_overflow_in __asan_memmove.zip

command to reproduce

```
./tifig -p -v [sample file] /dev/null
```

crash detail

```
==29736==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6110000d4687 at pc
0x0000004b4535 bp 0x7ffc7c0154e0 sp 0x7ffc7c014c90
READ of size 2891617427 at 0x6110000d4687 thread T0
    #0 0x4b4534 in __asan_memmove /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_interceptors_memintrinsics.cpp:30
    #1 0x5b3d50 in unsigned char* std::__copy_move<false, true,
std::random_access_iterator_tag>::__copy_m<unsigned char>(unsigned char const*, unsigned char
const*, unsigned char*) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_algobase.h:368:6
    #2 0x5b3d50 in unsigned char* std::__copy_move_a<false, unsigned char*, unsigned char*>
(unsigned char*, unsigned char*, unsigned char*) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_algobase.h:385:14
    #3 0x5b3d50 in unsigned char* std::__copy_move_a2<false, __gnu_cxx::__normal_iterator<unsigned
char*, std::vector<unsigned char, std::allocator<unsigned char> > >, unsigned char*>
(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, unsigned char*) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_algobase.h:422:18
    #4 0x5b3d50 in unsigned char* std::copy<__gnu_cxx::__normal_iterator<unsigned char*,
std::vector<unsigned char, std::allocator<unsigned char> > >, unsigned char*>
(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, unsigned char*) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_algobase.h:454:15
    #5 0x5b3d50 in unsigned char*
std::__uninitialized_copy<true>::__uninit_copy<__gnu_cxx::__normal_iterator<unsigned char*,
std::vector<unsigned char, std::allocator<unsigned char> > >, unsigned char*>
(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, unsigned char*) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_uninitialized.h:101:18
    #6 0x5b3d50 in unsigned char* std::uninitialized_copy<__gnu_cxx::__normal_iterator<unsigned
char*, std::vector<unsigned char, std::allocator<unsigned char> > >, unsigned char*>
(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, unsigned char*) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_uninitialized.h:131:14
    #7 0x5b3d50 in unsigned char*
std::__uninitialized_copy_a<__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned
char, std::allocator<unsigned char> > >, unsigned char*, unsigned char>
(__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, unsigned char*, std::allocator<unsigned char>&)
/usr/lib/gcc/x86_64-linux-gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_uninitialized.h:289:14
    #8 0x5b3d50 in void std::vector<unsigned char, std::allocator<unsigned char>
>::_M_range_insert<__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > > >(__gnu_cxx::__normal_iterator<unsigned char*,
std::vector<unsigned char, std::allocator<unsigned char> > >,
__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, std::forward_iterator_tag) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/vector.tcc:682:11
    #9 0x67e24d in void std::vector<unsigned char, std::allocator<unsigned char>
>::_M_insert_dispatch<__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > > >(__gnu_cxx::__normal_iterator<unsigned char*,
std::vector<unsigned char, std::allocator<unsigned char> > >,
__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, std::__false_type) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:1411:4
    #10 0x67e24d in __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > > std::vector<unsigned char, std::allocator<unsigned char>
>::insert<__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >, void>(__gnu_cxx::__normal_iterator<unsigned char const*,
std::vector<unsigned char, std::allocator<unsigned char> > >,
__gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char, std::allocator<unsigned
char> > >, __gnu_cxx::__normal_iterator<unsigned char*, std::vector<unsigned char,
std::allocator<unsigned char> > >) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:1132:4
    #11 0x67e24d in BitStream::read8BitsArray(std::vector<unsigned char, std::allocator<unsigned
char> >&, unsigned int) /home/bupt/Desktop/tifig/lib/heif/Srcs/common/bitstream.cpp:269:10
    #12 0x5f4b66 in HevcImageFileReader::getHevcItemData(std::vector<unsigned char,
std::allocator<unsigned char> > const&, std::vector<unsigned char, std::allocator<unsigned char>
>&) /home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:1584:19
    #13 0x5ee77b in HevcImageFileReader::getItemData(unsigned int, unsigned int,
std::vector<unsigned char, std::allocator<unsigned char> >&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:508:13
    #14 0x5fd6b3 in HevcImageFileReader::getItemDataWithDecoderParameters(unsigned int, unsigned
int, unsigned int, std::vector<unsigned char, std::allocator<unsigned char> >&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:770:5
    #15 0x5075ca in getImage(HevcImageFileReader&, unsigned int, unsigned int, Opts&)
/home/bupt/Desktop/tifig/src/loader.hpp:65:16
    #16 0x4feaf9 in convert(std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const&, Opts&) /home/bupt/Desktop/tifig/src/main.cpp:79:17
    #17 0x518b1a in main /home/bupt/Desktop/tifig/src/main.cpp:179:22
    #18 0x7fd207d3ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #19 0x422889 in _start (/home/bupt/Desktop/tifig/build/tifig+0x422889)

0x6110000d4687 is located 0 bytes to the right of 199-byte region [0x6110000d45c0,0x6110000d4687)
allocated by thread T0 here:
    #0 0x4faa18 in operator new(unsigned long) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:99
    #1 0x678295 in __gnu_cxx::new_allocator<unsigned char>::allocate(unsigned long, void const*)
/usr/lib/gcc/x86_64-linux-gnu/7.5.0/../../../../include/c++/7.5.0/ext/new_allocator.h:111:27
    #2 0x678295 in std::allocator_traits<std::allocator<unsigned char>
>::allocate(std::allocator<unsigned char>&, unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/alloc_traits.h:436:20
    #3 0x678295 in std::_Vector_base<unsigned char, std::allocator<unsigned char>
>::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:172:20
    #4 0x678295 in std::_Vector_base<unsigned char, std::allocator<unsigned char>
>::_M_create_storage(unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:187:33
    #5 0x678295 in std::_Vector_base<unsigned char, std::allocator<unsigned char>
>::_Vector_base(unsigned long, std::allocator<unsigned char> const&) /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:138:9
    #6 0x678295 in std::vector<unsigned char, std::allocator<unsigned char>
>::vector(std::vector<unsigned char, std::allocator<unsigned char> > const&) /usr/lib/gcc/x86_64-
linux-gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:327:9
    #7 0x678295 in BitStream::BitStream(std::vector<unsigned char, std::allocator<unsigned char> >
const&) /home/bupt/Desktop/tifig/lib/heif/Srcs/common/bitstream.cpp:28:5
    #8 0x6110000d4546  (<unknown module>)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:30 in __asan_memmove
Shadow bytes around the buggy address:
  0x0c2280012880: fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2280012890: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c22800128a0: 00 00 00 00 00 00 00 00 07 fa fa fa fa fa fa fa
  0x0c22800128b0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c22800128c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c22800128d0:[07]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c22800128e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c22800128f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2280012900: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2280012910: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2280012920: 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
  Shadow gap:              cc
==29736==ABORTING
```

Cvjark changed the title ~~Heap buffer overflow in~~ **Heap buffer overflow** on Jul 15

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant