New issue

Jump to bottom

heap-use-after-free in ~ItemInfoEntry() #70

Open **Cvjark** opened this issue on Jul 15 · 0 comments

Cvjark commented on Jul 15

crash sample

id17_heap-use-after-free_in_ItemInfoEntry.zip

command to reproduce

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

crash detail

```
==53276==ERROR: AddressSanitizer: heap-use-after-free on address 0x60c000000ac0 at pc
0x0000006a7b1c bp 0x7fff8406b050 sp 0x7fff8406b048
READ of size 8 at 0x60c000000ac0 thread T0
    #0 0x6a7b1b in ItemInfoEntry::~ItemInfoEntry()
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/iteminfobox.cpp:170:5
    #1 0x6a6899 in std::pair<unsigned int, ItemInfoEntry>::~pair() /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_pair.h:208:12
    #2 0x6a6899 in ItemInfoBox::addItemInfoEntry(ItemInfoEntry const&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/iteminfobox.cpp:47:5
    #3 0x6a6899 in ItemInfoBox::parseBox(BitStream&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/iteminfobox.cpp:109:9
    #4 0x6d3eb1 in MetaBox::parseBox(BitStream&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/metabox.cpp:242:26
    #5 0x5dbc4e in HevcImageFileReader::readStream()
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:1119:21
    #6 0x5cc52f in HevcImageFileReader::initialize(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:65:5
    #7 0x4fe834 in convert(std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const&, Opts&) /home/bupt/Desktop/tifig/src/main.cpp:49:12
    #8 0x518b1a in main /home/bupt/Desktop/tifig/src/main.cpp:179:22
    #9 0x7ff5564e3c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #10 0x422889 in _start (/home/bupt/Desktop/tifig/build/tifig+0x422889)
```

```
0x60c000000ac0 is located 0 bytes inside of 120-byte region [0x60c000000ac0,0x60c000000b38)
freed by thread T0 here:
    #0 0x4fb410 in operator delete(void*) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:160
    #1 0x6a781a in ItemInfoEntry::~ItemInfoEntry()
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/iteminfobox.cpp:170:5

previously 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 0x6a6d99 in ItemInfoEntry::parseBox(BitStream&)
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/iteminfobox.cpp:339:48

SUMMARY: AddressSanitizer: heap-use-after-free
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/iteminfobox.cpp:170:5 in
ItemInfoEntry::~ItemInfoEntry()
Shadow bytes around the buggy address:
  0x0c187fff8100: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa
  0x0c187fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c187fff8120: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c187fff8130: 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa
  0x0c187fff8140: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
=>0x0c187fff8150: fa fa fa fa fa fa fa fa[fd]fd fd fd fd fd fd fd
  0x0c187fff8160: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa
  0x0c187fff8170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c187fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c187fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c187fff81a0: 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
==53276==ABORTING
```

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant