monostream / tifig Public

New issue

Jump to bottom

SEGV in getType() #69

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

Cvjark commented on Jul 15

crash sample

id15_SEGV_in_getType.zip

command to reproduce

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

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==53234==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000c (pc 0x000000676063 bp
0x7ffe9f86b730 sp 0x7ffe9f86b5f0 T0)
==53234==The signal is caused by a READ memory access.
==53234==Hint: address points to the zero page.
    #0 0x676063 in Box::getType() const
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/bbox.cpp:44:12
    #1 0x6b06c5 in ItemPropertiesBox::getPropertyType(Box const*) const
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/itempropertiesbox.cpp:40:35
    #2 0x6b16b2 in ItemPropertiesBox::getItemProperties(unsigned int) const
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/itempropertiesbox.cpp:75:29
    #3 0x631106 in HevcImageFileReader::processItemProperties(unsigned int) const
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:1821:64
    #4 0x61437e in HevcImageFileReader::extractItems(MetaBox const&, unsigned int) const
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:1955:30
    #5 0x5dcfea in HevcImageFileReader::readStream()
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:1124:39
    #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 0x7f3dd101fc86 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)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/tifig/lib/heif/Srcs/common/bbox.cpp:44:12 in
Box::getType() const
==53234==ABORTING
```

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant