monostream / tifig Public

Code Issues 24 Pull requests 2 Actions Security Insights

New issue Jump to bottom

SEGV in this repo #71

Open Cvjark opened this issue on Jul 15 · 0 comments

Cvjark commented on Jul 15

sample file

id13_SEGV_in_size.zip

command to reproduce

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

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==74081==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000040 (pc 0x0000006c2382 bp
0x000000000038 sp 0x7ffe63ff83a0 T0)
==74081==The signal is caused by a READ memory access.
==74081==Hint: address points to the zero page.
    #0 0x6c2382 in std::vector<unsigned int, std::allocator<unsigned int> >::size() const
/usr/lib/gcc/x86_64-linux-gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h
    #1 0x6c2382 in std::vector<unsigned int, std::allocator<unsigned int>
>::vector(std::vector<unsigned int, std::allocator<unsigned int> > const&) /usr/lib/gcc/x86_64-
linux-gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h:327:19
    #2 0x6c2382 in SingleItemTypeReferenceBox::getToItemIds() const
/home/bupt/Desktop/tifig/lib/heif/Srcs/common/itemreferencebox.cpp:84:12
    #3 0x5efc25 in HevcImageFileReader::readItem(MetaBox const&, unsigned int,
std::vector<unsigned char, std::allocator<unsigned char> >&) const
/home/bupt/Desktop/tifig/lib/heif/Srcs/reader/hevcimagefilereader.cpp:2028:47
    #4 0x5ee016 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:475:13
    #5 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
    #6 0x5075ca in getImage(HevcImageFileReader&, unsigned int, unsigned int, Opts&)
/home/bupt/Desktop/tifig/src/loader.hpp:65:16
    #7 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
    #8 0x518b1a in main /home/bupt/Desktop/tifig/src/main.cpp:179:22
    #9 0x7f3180c46c86 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 /usr/lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/stl_vector.h in std::vector<unsigned int,
std::allocator<unsigned int> >::size() const
==74081==ABORTING
```

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant