New issue

Jump to bottom

Segmentation Fault error in read_image_band() of impex.hxx #494

⊙ Open **chooginlee** opened this issue on Mar 31, 2021 · 0 comments

chooginlee commented on Mar 31, 2021

Hello,

Using hugin (2020.0.0) software verdandi adopting vigra, I encountered on the segmentation fault error.
(http://hugin.sourceforge.net/releases/2020.0.0/en.shtml)

The root cause is assumed to be from
Illegal reference by `void vigra::StandardValueAccessor<unsigned short>::set<unsigned short, unsigned short*>(unsigned short, unsigned short*&).`
of debian package

> libvigraimpex-dev/focal,now 1.11.1+dfsg-7ubuntu1

The **set()** is assumed to be out-of-bound without any appropriate check of the valid address dereferenced by scanline.
See */include/vigra/impex.hxx:82-89*

lines;

```
                const ImageRowIterator is_end(is + width);

                while (is != is_end)
                {
                    image_accessor.set(*scanline, is);
                    scanline += offset;
                    ++is;
                }

                ++image_iterator.y;
```

The running command and backtrace is

```
oren@ubuntu:~$ sudo ./hugin-2020.0.0/build/src/tools/verdandi --output=1.tif ./poc
Warning: no TIFFTAG_SAMPLEFORMAT or TIFFTAG_DATATYPE, guessing pixeltype 'UINT16'.
Warning: no TIFFTAG_SAMPLEFORMAT or TIFFTAG_DATATYPE, guessing pixeltype 'UINT16'.
LogLuvSetupDecode: Inappropriate photometric interpretation 32985 for SGILog compression; must be either LogLUV or LogL.
ASAN:SIGSEGV
=================================================================
==100013==ERROR: AddressSanitizer: SEGV on unknown address 0x7fba4f4096f6 (pc 0x000000463ce6 bp 0x7fff40bb34e0 sp 0x7fff40bb33b0 T0)
    #0 0x463ce5 in void vigra::StandardValueAccessor<unsigned short>::set<unsigned short, unsigned short*>(unsigned short, unsigned short*&) const /usr/include/vigra/accessor.hxx:234
    #1 0x463ce5 in void vigra::detail::read_image_band<unsigned short, vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short> >(vigra::Decoder*, vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short>) /usr/include/vigra/impex.hxx:86
    #2 0x463ce5 in void vigra::detail::importImage<vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short> >(vigra::ImageImportInfo const&, vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short>, vigra::VigraTrueType) /usr/include/vigra/impex.hxx:212
    #3 0x60ef6c in void vigra::importImage<vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short> >(vigra::ImageImportInfo const&, vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short>) /usr/include/vigra/impex.hxx:796
    #4 0x60ef6c in void vigra::importImage<vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short> >(vigra::ImageImportInfo const&, std::pair<vigra::BasicImageIterator<unsigned short, unsigned short**>, vigra::StandardValueAccessor<unsigned short> >) /usr/include/vigra/impex.hxx:807
    #5 0x60ef6c in bool ResaveImage<vigra::BasicImage<unsigned short, std::allocator<unsigned short> >, vigra::BasicImage<unsigned short, std::allocator<unsigned short> > >(vigra::ImageImportInfo const&, vigra::ImageExportInfo&) /home/oren/hugin-2020.0.0/src/tools/verdandi.cpp:213
    #6 0x42154f in main /home/oren/hugin-2020.0.0/src/tools/verdandi.cpp:410
    #7 0x7fba574c682f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #8 0x424878 in _start (/home/oren/hugin-2020.0.0/build/src/tools/verdandi+0x424878)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /usr/include/vigra/accessor.hxx:234 void vigra::StandardValueAccessor<unsigned short>::set<unsigned short, unsigned short*>(unsigned short, unsigned short*&) const
==100013==ABORTING
```

poc.txt

I attached the poc file on this post.
Please kindly check the error.
Best,
Choongin Lee

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant