New issue

Jump to bottom

Out-of-memory in function tinyexr::DecodeEXRImage tinyexr.h:11046 #108

Closed **ChijinZ** opened this issue on Mar 4, 2019 · 0 comments

ChijinZ commented on Mar 4, 2019

I build tinyexr with clang and address sanitizer. When testcase (see: https://github.com/ChijinZ/security_advisories/blob/master/tinyexr_65f9859/crashes/out-of-memory-in-tinyexr.h:11046) is input into test_tinyexr (command: ./test_tinyexr testcase), a out-of-memory has triggered.

```
==28640==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x3f8000b80 bytes
    #0 0x4f2bb2 in operator new(unsigned long) (/home/jin/Documents/cve/tinyexr/test_tinyexr+0x4f2bb2)
    #1 0x54833a in __gnu_cxx::new_allocator<unsigned long>::allocate(unsigned long, void const*) /usr/bin/../lib/gcc/x86_64-linux-gnu/7.3.0/../../../../include/c++/7.3.0/ext/new_allocator.h:111:27
    #2 0x54833a in std::allocator_traits<std::allocator<unsigned long> >::allocate(std::allocator<unsigned long>&, unsigned long) /usr/bin/../lib/gcc/x86_64-linux-gnu/7.3.0/../../../../include/c++/7.3.0/bits/alloc_traits.h:436
    #3 0x54833a in std::_Vector_base<unsigned long, std::allocator<unsigned long> >::_M_allocate(unsigned long) /usr/bin/../lib/gcc/x86_64-linux-gnu/7.3.0/../../../../include/c++/7.3.0/bits/stl_vector.h:172
    #4 0x54833a in std::_Vector_base<unsigned long, std::allocator<unsigned long> >::_M_create_storage(unsigned long) /usr/bin/../lib/gcc/x86_64-linux-gnu/7.3.0/../../../../include/c++/7.3.0/bits/stl_vector.h:187
    #5 0x54833a in std::_Vector_base<unsigned long, std::allocator<unsigned long> >::_Vector_base(unsigned long, std::allocator<unsigned long> const&) /usr/bin/../lib/gcc/x86_64-linux-gnu/7.3.0/../../../../include/c++/7.3.0/bits/stl_vector.h:138
    #6 0x54833a in std::vector<unsigned long, std::allocator<unsigned long> >::vector(unsigned long, std::allocator<unsigned long> const&) /usr/bin/../lib/gcc/x86_64-linux-gnu/7.3.0/../../../../include/c++/7.3.0/bits/stl_vector.h:284
    #7 0x54833a in tinyexr::DecodeEXRImage(_EXRImage*, _EXRHeader const*, unsigned char const*, unsigned char const*, unsigned long, char const**) /home/jin/Documents/cve/tinyexr/./tinyexr.h:11046
    #8 0x54833a in LoadEXRImageFromMemory /home/jin/Documents/cve/tinyexr/./tinyexr.h:11625
    #9 0x52f88e in LoadEXRImageFromFile /home/jin/Documents/cve/tinyexr/./tinyexr.h:11602:10
    #10 0x522f17 in LoadEXR /home/jin/Documents/cve/tinyexr/./tinyexr.h:11161:15
    #11 0x58ee40 in main /home/jin/Documents/cve/tinyexr/test_tinyexr.cc:130:13
    #12 0x7f163a97fb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

==28640==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: out-of-memory (/home/jin/Documents/cve/tinyexr/test_tinyexr+0x4f2bb2) in operator new(unsigned long)
==28640==ABORTING
```

syoyo added a commit that referenced this issue on Mar 5, 2019

`Add check for invalid input value. Fixes #106 #107 #108 #109` 6c3b01f

syoyo closed this as completed on Mar 5, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants