New issue

Jump to bottom

Crash on DecodePixelData #124

Closed **strongcourage** opened this issue on Jul 7, 2019 · 0 comments

strongcourage commented on Jul 7, 2019

Hi,
Our fuzzer found a crash on tinyexr (the latest commit `2a5eac4` on master). I use your command to compile tinyexr as mentioned in #101 (clang++ version 4.0.0, Ubuntu 16.04 64 bit).
PoC: https://github.com/strongcourage/PoCs/blob/master/tinyexr_2a5eac4/PoC_iw_DecodePixelData
Command: test_tinyexr $POC
Valgrind says:

```
==4577== Invalid write of size 4
==4577==    at 0x4425B2: tinyexr::DecodePixelData(unsigned char**, int const*, unsigned char const*, unsigned long, int, int, int, int, int, int, int, int, unsigned long, unsigned
long, _EXRAttribute const*, unsigned long, _EXRChannelInfo const*, std::vector<unsigned long, std::allocator<unsigned long> > const&) [clone .isra.213] (tinyexr.h:9995)
==4577==    by 0x447CD8: tinyexr::DecodeChunk(_EXRImage*, _EXRHeader const*, std::vector<unsigned long long, std::allocator<unsigned long long> > const&, unsigned char const*,
unsigned long, std::string*) [clone .constprop.327] (tinyexr.h:10993)
==4577==    by 0x44C273: DecodeEXRImage (tinyexr.h:11190)
==4577==    by 0x44C273: LoadEXRImageFromMemory (tinyexr.h:11723)
==4577==    by 0x44D3A7: LoadEXRImageFromFile (tinyexr.h:11700)
==4577==    by 0x47B756: LoadEXR (tinyexr.h:11260)
==4577==    by 0x4022C2: main (test_tinyexr.cc:130)
==4577==  Address 0xffffff4005b1e960 is not stack'd, malloc'd or (recently) free'd
```

ASAN says:

```
tinyexr.h:10958:48: runtime error: signed integer overflow: 2147483647 + 1 cannot be represented in type 'int'
SUMMARY: AddressSanitizer: undefined-behavior tinyexr.h:10958:48 in
tinyexr.h:10961:39: runtime error: signed integer overflow: -2147483648 - 2147483647 cannot be represented in type 'int'
SUMMARY: AddressSanitizer: undefined-behavior tinyexr.h:10961:39 in
ASAN:DEADLYSIGNAL
=================================================================
==31934==ERROR: AddressSanitizer: SEGV on unknown address 0x6070000001c0 (pc 0x0000005de035 bp 0x7ffe6323ce30 sp 0x7ffe6323c380 T0)
==31934==The signal is caused by a WRITE memory access.
    #0 0x5de034 in tinyexr::DecodePixelData(unsigned char**, int const*, unsigned char const*, unsigned long, int, int, int, int, int, int, int, int, unsigned long, unsigned long,
_EXRAttribute const*, unsigned long, _EXRChannelInfo const*, std::vector<unsigned long, std::allocator<unsigned long> > const&) /home/dungnguyen/gueb-testing/tinyexr-
asan/./tinyexr.h:9995:22
    #1 0x5b64fd in tinyexr::DecodeChunk(_EXRImage*, _EXRHeader const*, std::vector<unsigned long long, std::allocator<unsigned long long> > const&, unsigned char const*, unsigned
long, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >*) /home/dungnguyen/gueb-testing/tinyexr-asan/./tinyexr.h:10984:20
    #2 0x585b35 in tinyexr::DecodeEXRImage(_EXRImage*, _EXRHeader const*, unsigned char const*, unsigned char const*, unsigned long, char const**) /home/dungnguyen/gueb-
testing/tinyexr-asan/./tinyexr.h:11190:15
    #3 0x5826fe in LoadEXRImageFromMemory /home/dungnguyen/gueb-testing/tinyexr-asan/./tinyexr.h:11722:10
    #4 0x5689e1 in LoadEXRImageFromFile /home/dungnguyen/gueb-testing/tinyexr-asan/./tinyexr.h:11699:10
    #5 0x55de1e in LoadEXR /home/dungnguyen/gueb-testing/tinyexr-asan/./tinyexr.h:11260:15
    #6 0x5bd092 in main /home/dungnguyen/gueb-testing/tinyexr-asan/test_tinyexr.cc:130:13
    #7 0x7fdba826082f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #8 0x41b878 in _start (/home/dungnguyen/PoCs/tinyexr_2a5eac4/test_tinyexr-asan+0x41b878)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/dungnguyen/gueb-testing/tinyexr-asan/./tinyexr.h:9995:22 in tinyexr::DecodePixelData(unsigned char**, int const*, unsigned char const*,
unsigned long, int, int, int, int, int, int, int, int, unsigned long, unsigned long, _EXRAttribute const*, unsigned long, _EXRChannelInfo const*, std::vector<unsigned long,
std::allocator<unsigned long> > const&)
==31934==ABORTING
```

Thanks,
Manh Dung

syoyo closed this as completed in a685e33 on Jul 7, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant