New issue

Jump to bottom

A stack-buffer-overflow in paramset.h:56 with default test case #296

Open seviezhou opened this issue on Aug 4, 2020 · 0 comments

seviezhou commented on Aug 4, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), pbrt (latest master aaa552)

Configure

cmake ../srcs -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address"

Command line

./build/pbrt --quick ./scenes/killeroo-simple.pbrt --outfile /tmp/pbrt

AddressSanitizer output

```
=================================================================
==36886==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffec8b190e0 at pc 0x0000006463fc bp 0x7ffec8b17c80 sp 0x7ffec8b17c70
WRITE of size 8 at 0x7ffec8b190e0 thread T0
    #0 0x6463fb in std::_Vector_base<std::shared_ptr<pbrt::ParamSetItem<bool> >, std::allocator<std::shared_ptr<pbrt::ParamSetItem<bool> > > >::_Vector_impl::_Vector_impl()
/usr/include/c++/5/bits/stl_vector.h:87
    #1 0x6463fb in std::_Vector_base<std::shared_ptr<pbrt::ParamSetItem<bool> >, std::allocator<std::shared_ptr<pbrt::ParamSetItem<bool> > > >::_Vector_base()
/usr/include/c++/5/bits/stl_vector.h:125
    #2 0x6463fb in std::vector<std::shared_ptr<pbrt::ParamSetItem<bool> >, std::allocator<std::shared_ptr<pbrt::ParamSetItem<bool> > > >::vector()
/usr/include/c++/5/bits/stl_vector.h:257
    #3 0x6463fb in pbrt::ParamSet::ParamSet() /home/seviezhou/pbrt/src/core/paramset.h:56
    #4 0x6463fb in parseParams<std::function<pbrt::string_view(int)>, pbrt::parse(std::unique_ptr<pbrt::Tokenizer>)::<lambda(pbrt::string_view)> >
/home/seviezhou/pbrt/src/core/parser.cpp:714
    #5 0x65e390 in operator() /home/seviezhou/pbrt/src/core/parser.cpp:848
    #6 0x65e390 in parse /home/seviezhou/pbrt/src/core/parser.cpp:909
    #7 0x666aca in pbrt::pbrtParseFile(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >) /home/seviezhou/pbrt/src/core/parser.cpp:1101
    #8 0x48cb36 in main /home/seviezhou/pbrt/src/main/pbrt.cpp:169
    #9 0x7f6786b2b83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #10 0x4a9538 in _start (/home/seviezhou/pbrt/build/pbrt+0x4a9538)

Address 0x7ffec8b190e0 is located in stack of thread T0 at offset 3232 in frame
    #0 0x65784f in parse /home/seviezhou/pbrt/src/core/parser.cpp:786

  This frame has 93 object(s):
    [64, 65) 'ungetTokenSet'
    [128, 132) '__args#0'
    [192, 196) '__args#0'
    [256, 260) '__args#0'
    [320, 324) '__args#0'
    [384, 388) '__args#0'
    [448, 452) '__args#0'
    [512, 516) '__args#0'
    [576, 580) '__args#0'
    [640, 644) '__args#0'
    [704, 708) '__args#0'
    [768, 772) '__args#0'
    [832, 836) '__args#0'
    [896, 900) '__args#0'
    [960, 964) '__args#0'
    [1024, 1028) '__args#0'
    [1088, 1092) '__args#0'
    [1152, 1156) '__args#0'
    [1216, 1220) '__args#0'
    [1280, 1284) '__args#0'
    [1344, 1348) '__args#0'
    [1408, 1412) '__args#0'
    [1472, 1476) '__args#0'
    [1536, 1540) '__args#0'
    [1600, 1604) '__args#0'
    [1664, 1668) '__args#0'
    [1728, 1732) '__args#0'
    [1792, 1796) '__args#0'
    [1856, 1860) '__args#0'
    [1920, 1928) '__dnew'
    [1984, 1992) '__dnew'
    [2048, 2056) '__dnew'
    [2112, 2120) '__dnew'
    [2176, 2184) '__dnew'
    [2240, 2248) '__dnew'
    [2304, 2312) '__dnew'
    [2368, 2376) '__dnew'
    [2432, 2440) '__dnew'
    [2496, 2504) '__dnew'
    [2560, 2568) '__dnew'
    [2624, 2632) '__dnew'
    [2688, 2696) '__dnew'
    [2752, 2760) '__dnew'
    [2816, 2824) '__dnew'
    [2880, 2896) 'ungetToken'
    [2944, 2968) 'fileStack'
    [3008, 3032) 'basicParamListEntrypoint'
    [3072, 3200) 'arena'
    [3264, 3496) 'params' <== Memory access at offset 3232 underflows this variable
    [3552, 3816) 'params'
    [3872, 4136) 'params'
```

```
    [4192, 4456) 'params'
    [4512, 4776) 'params'
    [4832, 4840) 'v'
    [4896, 4908) 'v'
    [4960, 4976) 'v'
    [5024, 5056) 'ungetTokenValue'
    [5088, 5120) 'nextToken'
    [5152, 5184) '<unknown>'
    [5216, 5248) '<unknown>'
    [5280, 5312) '<unknown>'
    [5344, 5376) '<unknown>'
    [5408, 5440) '<unknown>'
    [5472, 5504) '<unknown>'
    [5536, 5568) '<unknown>'
    [5600, 5632) '<unknown>'
    [5664, 5696) '<unknown>'
    [5728, 5760) '<unknown>'
    [5792, 5824) '<unknown>'
    [5856, 5888) '<unknown>'
    [5920, 5952) 'n'
    [5984, 6016) '<unknown>'
    [6048, 6080) '<unknown>'
    [6112, 6144) 'n'
    [6176, 6208) '<unknown>'
    [6240, 6272) '<unknown>'
    [6304, 6336) '<unknown>'
    [6368, 6400) 'n'
    [6432, 6464) '<unknown>'
    [6496, 6528) '<unknown>'
    [6560, 6592) '<unknown>'
    [6624, 6656) '<unknown>'
    [6688, 6720) '<unknown>'
    [6752, 6784) '<unknown>'
    [6816, 6848) '<unknown>'
    [6880, 6912) 'n'
    [6944, 6976) '<unknown>'
    [7008, 7040) '<unknown>'
    [7072, 7104) 'n'
    [7136, 7168) 'filename'
    [7200, 7232) '<unknown>'
    [7264, 7300) 'v'
    [7360, 7424) 'm'
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /usr/include/c++/5/bits/stl_vector.h:87 std::_Vector_base<std::shared_ptr<pbrt::ParamSetItem<bool> >,
std::allocator<std::shared_ptr<pbrt::ParamSetItem<bool> > > >::_Vector_impl::_Vector_impl()
Shadow bytes around the buggy address:
  0x10005915b1c0: 00 f4 f4 f4 f2 f2 f2 f2 00 f4 f4 f4 f2 f2 f2 f2
  0x10005915b1d0: 00 f4 f4 f4 f2 f2 f2 f2 00 f4 f4 f4 f2 f2 f2 f2
  0x10005915b1e0: 00 f4 f4 f4 f2 f2 f2 f2 00 f4 f4 f4 f2 f2 f2 f2
  0x10005915b1f0: 00 00 f4 f4 f2 f2 f2 f2 00 00 00 f4 f2 f2 f2 f2
  0x10005915b200: 00 00 00 f4 f2 f2 f2 f2 00 00 00 00 00 00 00 00
=>0x10005915b210: 00 00 00 00 00 00 00 00 f2 f2 f2 f2[f2]f2 f2 f2
  0x10005915b220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005915b230: 00 00 00 00 00 00 00 00 00 00 00 00 00 f4 f4 f4
  0x10005915b240: f2 f2 f2 f2 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005915b250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005915b260: 00 00 00 00 00 f4 f4 f4 f2 f2 f2 f2 00 00 00 00
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==36886==ABORTING
```

POC

stack-overflow-ParamSet-paramset-56.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant