New issue

Jump to bottom

A heap overflow in peglib.h:347 #122

Closed **seviezhou** opened this issue on Aug 7, 2020 · 9 comments

seviezhou commented on Aug 7, 2020

System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), peglint (latest master 14305f)

Configure

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

Command line

./build/lint/peglint --ast --opt ./heap-overflow-resolve_escape_sequence-peglib-347 ./pl0/samples/fib.pas

AddressSanitizer output

```
=================================================================
==23131==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61a00001f71b at pc 0x000000459cbd bp 0x7ffc8a717b10 sp 0x7ffc8a717b00
READ of size 1 at 0x61a00001f71b thread T0
    #0 0x459cbc in peg::resolve_escape_sequence[abi:cxx11](char const*, unsigned long) /home/seviezhou/cpppeglib/lint/../peglib.h:347
    #1 0x45a12a in peg::ParserGenerator::setup_actions()::{lambda(peg::SemanticValues const&)#18}::operator()[abi:cxx11](peg::SemanticValues const&) const
/home/seviezhou/cpppeglib/lint/../peglib.h:3304
    #2 0x45a12a in std::_Function_handler<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > (peg::SemanticValues const&),
peg::ParserGenerator::setup_actions()::{lambda(peg::SemanticValues const&)#18}>::_M_invoke(std::_Any_data const&, peg::SemanticValues const&) /usr/include/c++/5/functional:1857
    #3 0x4fb935 in std::function<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > (peg::SemanticValues const&)>::operator()(peg::SemanticValues
const&) const /usr/include/c++/5/functional:2267
    #4 0x4fb935 in peg::any peg::call<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >, std::function<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > (peg::SemanticValues const&)>, (decltype(nullptr))0, peg::SemanticValues&>(std::function<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > (peg::SemanticValues const&)>, peg::SemanticValues&) /home/seviezhou/cpppeglib/lint/../peglib.h:631
    #5 0x4fb935 in peg::Action::TypeAdaptor_csv<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > >::operator()(peg::SemanticValues&, peg::any&)
/home/seviezhou/cpppeglib/lint/../peglib.h:691
    #6 0x4fb935 in std::_Function_handler<peg::any (peg::SemanticValues&, peg::any&), peg::Action::TypeAdaptor_csv<std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > >::_M_invoke(std::_Any_data const&, peg::SemanticValues&, peg::any&) /usr/include/c++/5/functional:1857
    #7 0x4904d6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x4904d6)
    #8 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>(char
const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1})
/home/seviezhou/cpppeglib/lint/../peglib.h:880
    #9 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #10 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #11 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #12 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #13 0x4a90fa in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #14 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #15 0x4ddae7 in peg::PrioritizedChoice::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const
/home/seviezhou/cpppeglib/lint/../peglib.h:1058
    #16 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #17 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #18 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #19 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #20 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #21 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #22 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #23 0x4a933a in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #24 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #25 0x4df989 in peg::Repetition::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1125
    #26 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #27 0x469b21 in peg::TokenBoundary::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2464
    #28 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #29 0x4a95d1 in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #30 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #31 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #32 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #33 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #34 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #35 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #36 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #37 0x4ddae7 in peg::PrioritizedChoice::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const
/home/seviezhou/cpppeglib/lint/../peglib.h:1058
    #38 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #39 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #40 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #41 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #42 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #43 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #44 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #45 0x4a90fa in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #46 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #47 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #48 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #49 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #50 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #51 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #52 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #53 0x4a933a in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #54 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #55 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #56 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #57 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #58 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #59 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #60 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #61 0x4df989 in peg::Repetition::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1125
```

```
    #62 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #63 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #64 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #65 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #66 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #67 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #68 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #69 0x4a90fa in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #70 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #71 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #72 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #73 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #74 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #75 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #76 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #77 0x4a961a in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #78 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #79 0x4ddae7 in peg::PrioritizedChoice::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const
/home/seviezhou/cpppeglib/lint/../peglib.h:1058
    #80 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #81 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #82 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #83 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #84 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #85 0x48c29c in peg::WeakHolder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1450
    #86 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #87 0x4df989 in peg::Repetition::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1125
    #88 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #89 0x4a92e6 in peg::Sequence::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:1010
    #90 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #91 0x48ffa6 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}::operator()(peg::any&) const
(/home/seviezhou/cpppeglib/build/lint/peglint+0x48ffa6)
    #92 0x50d5f4 in void peg::Context::packrat<peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::{lambda(peg::any&)#1}>
(char const*, unsigned long, unsigned long&, peg::any&, peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const::
{lambda(peg::any&)#1}) /home/seviezhou/cpppeglib/lint/../peglib.h:880
    #93 0x50d5f4 in peg::Holder::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2532
    #94 0x45be13 in peg::Ope::parse(char const*, unsigned long, peg::SemanticValues&, peg::Context&, peg::any&) const /home/seviezhou/cpppeglib/lint/../peglib.h:2440
    #95 0x512115 in peg::Definition::parse_core(char const*, unsigned long, peg::SemanticValues&, peg::any&, char const*) const /home/seviezhou/cpppeglib/lint/../peglib.h:2345
    #96 0x527a1a in peg::Definition::parse(char const*, unsigned long, peg::any&, char const*) const /home/seviezhou/cpppeglib/lint/../peglib.h:2227
    #97 0x527a1a in peg::ParserGenerator::perform_core(char const*, unsigned long, std::unordered_map<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>
>, std::shared_ptr<peg::Ope>, std::hash<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::equal_to<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const,
std::shared_ptr<peg::Ope> > > > const&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&, std::function<void (unsigned long, unsigned long,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)>) /home/seviezhou/cpppeglib/lint/../peglib.h:3396
    #98 0x557b83 in peg::ParserGenerator::parse(char const*, unsigned long, std::unordered_map<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::shared_ptr<peg::Ope>, std::hash<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::equal_to<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const,
std::shared_ptr<peg::Ope> > > > const&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&, std::function<void (unsigned long, unsigned long,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)>) /home/seviezhou/cpppeglib/lint/../peglib.h:2880
    #99 0x557b83 in peg::parser::load_grammar(char const*, unsigned long, std::unordered_map<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::shared_ptr<peg::Ope>, std::hash<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::equal_to<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const,
std::shared_ptr<peg::Ope> > > > const&) /home/seviezhou/cpppeglib/lint/../peglib.h:3850
    #100 0x557b83 in peg::parser::load_grammar(char const*, unsigned long) /home/seviezhou/cpppeglib/lint/../peglib.h:3855
    #101 0x429e66 in main /home/seviezhou/cpppeglib/lint/peglint.cc:111
    #102 0x7fc56923a83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #103 0x42b888 in _start (/home/seviezhou/cpppeglib/build/lint/peglint+0x42b888)

0x61a00001f71b is located 0 bytes to the right of 1179-byte region [0x61a00001f280,0x61a00001f71b)
allocated by thread T0 here:
    #0 0x7fc569e95532 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99532)
    #1 0x46139e in __gnu_cxx::new_allocator<char>::allocate(unsigned long, void const*) /usr/include/c++/5/ext/new_allocator.h:104
    #2 0x46139e in std::allocator_traits<std::allocator<char> >::allocate(std::allocator<char>&, unsigned long) /usr/include/c++/5/bits/alloc_traits.h:491
    #3 0x46139e in std::_Vector_base<char, std::allocator<char> >::_M_allocate(unsigned long) /usr/include/c++/5/bits/stl_vector.h:170
    #4 0x46139e in std::vector<char, std::allocator<char> >::_M_default_append(unsigned long) /usr/include/c++/5/bits/vector.tcc:557
    #5 0x46139e in std::vector<char, std::allocator<char> >::resize(unsigned long) /usr/include/c++/5/bits/stl_vector.h:676
    #6 0x46139e in read_file(char const*, std::vector<char, std::allocator<char> >&) /home/seviezhou/cpppeglib/lint/peglint.cc:18

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/cpppeglib/lint/../peglib.h:347 peg::resolve_escape_sequence[abi:cxx11](char const*, unsigned long)
Shadow bytes around the buggy address:
  0x0c347fffbe90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbeb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fffbed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c347fffbee0: 00 00 00[03]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fffbf30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==23131==ABORTING
```

yhirose commented on Aug 7, 2020 — Owner

@seviezhou, thanks for the feedback. Could you give me more detailed information about it? Thanks!

seviezhou commented on Aug 7, 2020 — Author

Well, this bug is found by fuzzing. I compiled the code with Address Sanitizer and mutate the `pl0.peg` sample file in the project. I use this command to execute the program. After some mutation, I got this crash, I think you can reproduce it using the command and input I give.

I am sorry, I am not very familiar with the project code, so I cannot analyze the actually cause of this bug.

yhirose commented on Aug 7, 2020 — Owner

@seviezhou, ok. How did you mutate the pl0.peg?

seviezhou commented on Aug 7, 2020 — Author

Just some randomly bit/byte flipping, or substitute some parts of inputs with a set of predefined strings.

yhirose commented on Aug 7, 2020 — Owner

@seviezhou, does it mean that the mutated file is no longer a valid text UTF-8 file?

seviezhou commented on Aug 7, 2020 — Author

It is possible that some part of the mutated file is not valid text file, but for this case, you can see that most of the content is still text, and the bug was triggered by these text content:

```
program    <- _ block '.' _

block      <- const var procedure statement
const      <- ('CONST' __ ident '=' _ number (',' _ ident '=' _ number)* ';' _)?
var        <- ('VAR' __ ident (',' _ ident)* ';' _)?
procedure  <- ('PROCEDURE' __ ident ';' _ block ';' _)*

statement  <- (assignment / call / statements / if / while / out / in)?
assignment <- ident ':=' _ expression
call       <- 'CALL' __ ident
statements <- 'BEGIN' __ statement (';' _ statement )* 'END' __
if         <- 'IF' __ condition 'THEN' __ statement
while      <- 'WHILE' __ condition 'DO' __ statement
out        <- ('out' __ / 'write' __ / '!' _) expression
in         <- ('in' __ / 'read' __ / '?' _) ident

condition  <- odd / compare
odd        <- 'ODD' __ expression
compare    <- expression compare_op expression
compare_op <- < '=' / '#' / '<=' / '<' / '>=' / '>' > _

expression <- sign term (term_op term)*
sign       <- < [-+]? > _
term_op    <- < [-+] > _

term       <- factor (factor_op factor)*
factor_op  <- < [*/] > _

factor     <- ident / number / '(' _ expression ')' _

ident      <- < [a-z] [a-z0-9]* > _
number     <- < [0-9]+ > _

~_         <- [ \t\r\n]*
~__        <- ![a-z0-9_
```

yhirose commented on Aug 7, 2020 — Owner

@seviezhou, thanks for the info!

seviezhou commented on Aug 7, 2020 — Author

I'm glad that it helps.

yhirose closed this as completed in b3b29ce on Aug 7, 2020

fgeek commented on Jul 20, 2021

CVE-2020-23915 has been assigned for this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants