A Segmentation fault in peglib.h:3650 #121

Closed **seviezhou** opened this issue on Aug 7, 2020 · 5 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 @@ ./pl0/samples/fib.pas

Output

```
Segmentation fault
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==67168==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000000d8 (pc 0x000000504159 bp 0x0fffe1f65aa4 sp 0x7fff0fb2d380 T0)
    #0 0x504158 in std::vector<std::shared_ptr<peg::AstBase<peg::EmptyType> >, std::allocator<std::shared_ptr<peg::AstBase<peg::EmptyType> > > >::size() const
/usr/include/c++/5/bits/stl_vector.h:655
    #1 0x504158 in std::shared_ptr<peg::AstBase<peg::EmptyType> > peg::AstOptimizer::optimize<peg::AstBase<peg::EmptyType> >(std::shared_ptr<peg::AstBase<peg::EmptyType> >,
std::shared_ptr<peg::AstBase<peg::EmptyType> >) /home/seviezhou/cpppeglib/lint/../peglib.h:3650
    #2 0x42aa14 in main /home/seviezhou/cpppeglib/lint/peglint.cc:178
    #3 0x7fe349ce283f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #4 0x42b888 in _start (/home/seviezhou/cpppeglib/build/lint/peglint+0x42b888)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /usr/include/c++/5/bits/stl_vector.h:655 std::vector<std::shared_ptr<peg::AstBase<peg::EmptyType> >,
std::allocator<std::shared_ptr<peg::AstBase<peg::EmptyType> > > >::size() const
==67168==ABORTING
```

POC

SEGV-optimize-peglib-3650.zip

yhirose commented on Aug 7, 2020 Owner

@seviezhou, thanks for the feedback. I couldn't reproduce it on my machine.

```
> ./build/lint/peglint --ast --opt @@ ./pl0/samples/fib.pas
can't open the grammar file.
```

What do you think I am missing to reproduce it? Thanks!

seviezhou commented on Aug 7, 2020 Author

You should replace `@@` with the file I attached:

```
./build/lint/peglint --ast --opt ./SEGV-optimize-peglib-3650 ./pl0/samples/fib.pas
```

yhirose closed this as completed in `0061f39` on Aug 7, 2020

fgeek commented on Jul 20, 2021

CVE-2020-23914 has been assigned for this issue.

fgeek commented on Jul 20, 2021

@seviezhou you should give afl or other program used in fuzzing credit in advisories.

seviezhou commented on Jul 20, 2021 Author

> **@seviezhou** you should give afl or other program used in fuzzing credit in advisories.

It is found by a fuzzer built by us, it has not become open source yet.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants