ethereum / solidity Public

Code · Issues 1k · Pull requests 40 · Actions · Projects 6 · Security · •••

New issue

Jump to bottom

[SMTChecker] ICE in `SMTEncoder::indexOrMemberAssignment()` with public state variable with invalid double initialization #12973

Open pietroborrello opened this issue on Apr 29 · 2 comments

Labels	bug 🐛 should compile without error SMT
Projects	SMT Checker

pietroborrello commented on Apr 29

Describe the bug

The attached testcase crashes the solidity compiler solc with an InternalCompilerError: Solidity assertion failed in in solidity::frontend::SMTEncoder::indexOrMemberAssignment

solidity/libsolidity/formal/SMTEncoder.cpp
Line 1596 in `b35cda5`

```
1596        solAssert(symbStruct, "");
```

To Reproduce

Built solc_ossfuzz using clang-10 according to the oss-fuzz script with `CXXFLAGS='-O1 -fsanitize=address -fsanitize=array-bounds,bool,builtin,enum,float-divide-by-zero,function,integer-divide-by-zero,null,object-size,return,returns-nonnull-attribute,shift,signed-integer-overflow,unreachable,vla-bound,vptr'`

commit: `b35cda5`

Crash Output

```
$ ./solc_ossfuzz id:000000,sig:06,src:012925,time:33170510,op:havoc,rep:2,trial:3
INFO: Seed: 2663119797
INFO: Loaded 1 modules   (537599 inline 8-bit counters): 537599 [0x53258a0, 0x53a8c9f),
INFO: Loaded 1 PC tables (537599 PCs): 537599 [0x53a8ca0,0x5bdcc90),
solc_ossfuzz: Running 1 inputs 1 time(s) each.
```

```
Running: id:000000,sig:06,src:012925,time:33170510,op:havoc,rep:2,trial:3
terminate called after throwing an instance of
'boost::wrapexcept<solidity::langutil::InternalCompilerError>'
  what():  Solidity assertion failed
==2678862== ERROR: libFuzzer: deadly signal
    #0 0x505691 in __sanitizer_print_stack_trace (solc_ossfuzz+0x505691)
    #1 0x55da28 in fuzzer::PrintStackTrace() (solc_ossfuzz+0x55da28)
    #2 0x542819 in fuzzer::Fuzzer::CrashCallback() (solc_ossfuzz+0x542819)
    #3 0x7ffff7c713bf  (/lib/x86_64-linux-gnu/libpthread.so.0+0x143bf)
    #4 0x7ffff7a8103a in __libc_signal_restore_set /build/glibc-sMfBJT/glibc-
2.31/signal/../sysdeps/unix/sysv/linux/internal-signals.h:86:3
    #5 0x7ffff7a8103a in raise /build/glibc-sMfBJT/glibc-
2.31/signal/../sysdeps/unix/sysv/linux/raise.c:48:3
    #6 0x7ffff7a60858 in abort /build/glibc-sMfBJT/glibc-2.31/stdlib/abort.c:79:7
    #7 0x7ffff7e6d910  (/lib/x86_64-linux-gnu/libstdc++.so.6+0x9e910)
    #8 0x7ffff7e7938b  (/lib/x86_64-linux-gnu/libstdc++.so.6+0xaa38b)
    #9 0x7ffff7e793f6 in std::terminate() (/lib/x86_64-linux-gnu/libstdc++.so.6+0xaa3f6)
    #10 0x7ffff7e796a8 in __cxa_throw (/lib/x86_64-linux-gnu/libstdc++.so.6+0xaa6a8)
    #11 0x6407ae in void boost::throw_exception<solidity::langutil::InternalCompilerError>
(solidity::langutil::InternalCompilerError const&) (solc_ossfuzz+0x6407ae)
    #12 0x181c97c in
solidity::frontend::SMTEncoder::indexOrMemberAssignment(solidity::frontend::Expression const&,
solidity::smtutil::Expression const&) (solc_ossfuzz+0x181c97c)
    #13 0x1809c94 in solidity::frontend::SMTEncoder::assignment(solidity::frontend::Expression
const&, solidity::smtutil::Expression const&, solidity::frontend::Type const*)
(solc_ossfuzz+0x1809c94)
    #14 0x17ffc41 in solidity::frontend::SMTEncoder::endVisit(solidity::frontend::Assignment
const&) (solc_ossfuzz+0x17ffc41)
    #15 0x169761d in
solidity::frontend::CHC::defineContractInitializer(solidity::frontend::ContractDefinition const&,
solidity::frontend::ContractDefinition const&) (solc_ossfuzz+0x169761d)
    #16 0x168eca6 in solidity::frontend::CHC::endVisit(solidity::frontend::ContractDefinition
const&) (solc_ossfuzz+0x168eca6)
    #17 0xe66f1a in void
solidity::frontend::ASTNode::listAccept<std::shared_ptr<solidity::frontend::ASTNode> >
(std::vector<std::shared_ptr<solidity::frontend::ASTNode>,
std::allocator<std::shared_ptr<solidity::frontend::ASTNode> > > const&,
solidity::frontend::ASTConstVisitor&) (solc_ossfuzz+0xe66f1a)
    #18 0xe66985 in solidity::frontend::SourceUnit::accept(solidity::frontend::ASTConstVisitor&)
const (solc_ossfuzz+0xe66985)
    #19 0x167c1d9 in solidity::frontend::CHC::analyze(solidity::frontend::SourceUnit const&)
(solc_ossfuzz+0x167c1d9)
    #20 0x178e5f3 in solidity::frontend::ModelChecker::analyze(solidity::frontend::SourceUnit
const&) (solc_ossfuzz+0x178e5f3)
    #21 0x88c1f2 in solidity::frontend::CompilerStack::analyze() (solc_ossfuzz+0x88c1f2)
    #22 0x892357 in
solidity::frontend::CompilerStack::compile(solidity::frontend::CompilerStack::State)
(solc_ossfuzz+0x892357)
    #23 0x56b6d5 in FuzzerUtil::testCompiler(std::map<std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::less<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::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > > > >&, bool, unsigned int, bool, bool) (solc_ossfuzz+0x56b6d5)
    #24 0x562ddf in LLVMFuzzerTestOneInput (solc_ossfuzz+0x562ddf)
    #25 0x543f49 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long)
(solc_ossfuzz+0x543f49)
    #26 0x52ee49 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long)
(solc_ossfuzz+0x52ee49)
    #27 0x533d52 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned
long)) (solc_ossfuzz+0x533d52)
    #28 0x52ebd2 in main (solc_ossfuzz+0x52ebd2)
    #29 0x7ffff7a620b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #30 0x48440d in _start (solc_ossfuzz+0x48440d)

NOTE: libFuzzer has rudimentary signal handlers.
      Combine libFuzzer with AddressSanitizer or similar for better crash reports.
SUMMARY: libFuzzer: deadly signal
```

zipped testcase to reproduce:
id:000000,sig:06,src:012925,time:33170510,op:havoc,rep:2,trial:3.zip

cameel commented on Apr 30 Member

Thanks for the report! I can confirm that this is reproducible on 0.8.13. Here's a slightly cleaned up repro:

```
contract C {
    string public name = (C).name = type(C).name;
}
```

```
solc test.sol --model-checker-engine all
```

```
Internal compiler error:
/solidity/libsolidity/formal/SMTEncoder.cpp(1596): Throw in function void
solidity::frontend::SMTEncoder::indexOrMemberAssignment(const solidity::frontend::Expression&,
const solidity::smtutil::Expression&)
Dynamic exception type: boost::wrapexcept<solidity::langutil::InternalCompilerError>
std::exception::what: Solidity assertion failed
[solidity::util::tag_comment*] = Solidity assertion failed
```

By the way, **@pietroborrello** if the Solidity sample is not huge, its best to just include it directly in the bug report. Also, if you run the sample though solc and that triggers an Internal Compiler Error (like I did above) that's a much simpler starting point and enough for us to investigate, no need to post the whole fuzzer output in that case. In any case thanks again for taking your time to report this!

cameel added bug 🐛 **should compile without error** labels on Apr 30

cameel added this to **New issues** in **Solidity** via automation on Apr 30

cameel added this to **To Do** in **SMT Checker** via automation on Apr 30

cameel changed the title ~~InternalCompilerError: Solidity assertion failed in in solidity::frontend::SMTEncoder::indexOrMemberAssignment~~ [SMTChecker] ICE in `SMTEncoder::indexOrMemberAssignment()` with public state variable with invalid double initialization on Apr 30

pietroborrello commented on May 2 Author

Thank you for looking into this and for your kind reply. Next time I will follow your guidelines to ease your work :)

👍 1

leonardoalt moved this from **To Do** to **High priority** in **SMT Checker** on May 17

NunoFilipeSantos added the SMT label 9 days ago

Assignees

No one assigned

Labels

bug 🐛 should compile without error SMT

Projects

SMT Checker

High priority

Milestone

No milestone

Development

No branches or pull requests

3 participants