Starred by 2 users

Owner:	----
CC:	chris...@ethereum.org bharg...@ethereum.org marti...@ethereum.org a...@ethereum.org
Status:	Verified *(Closed)*
Components:	----
Modified:	Jan 8, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Engine-afl
Fuzz-Blocker
Security_Severity-High
Proj-solidity
Reported-2020-11-05
Disclosure-2021-02-03

Issue 26997: solidity:solc_noopt_ossfuzz: Stack-use-after-return in solidity::smtutil::CHCSmtLib2Interface::querySolver

Reported by ClusterFuzz-External on Thu, Nov 5, 2020, 9:05 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5750916210491392

Project: solidity
Fuzzing Engine: afl
Fuzz Target: solc_noopt_ossfuzz
Job Type: afl_asan_solidity
Platform Id: linux

Crash Type: Stack-use-after-return READ 8
Crash Address: 0x7f51b1689128
Crash State:
  solidity::smtutil::CHCSmtLib2Interface::querySolver
  solidity::smtutil::CHCSmtLib2Interface::query
  solidity::frontend::CHC::query

Sanitizer: address (ASAN)

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_solidity&range=202011040618:202011050621

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5750916210491392

Issue filed automatically.

See https://google.github.io/oss-fuzz/advanced-topics/reproducing for instructions to reproduce this bug locally.
When you fix this bug, please
  * mention the fix revision(s).
  * state whether the bug was a short-lived regression or an old bug in any stable releases.
  * add any other useful information.
This information can help downstream consumers.

If you need to contact the OSS-Fuzz team with a question, concern, or any other feedback, please file an issue at https://github.com/google/oss-fuzz/issues. Comments on individual Monorail issues are not monitored.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse
without an upstream patch, then the bug report will automatically
become visible to the public.

Comment 1 by sheriffbot on Thu, Nov 5, 2020, 3:05 PM EST Project Member

Labels: Disclosure-2021-02-03

Comment 2 by ClusterFuzz-External on Fri, Nov 6, 2020, 5:08 AM EST Project Member

Labels: Fuzz-Blocker

This crash occurs very frequently on linux platform and is likely preventing the fuzzer solc_noopt_ossfuzz from making much progress. Fixing this will allow more bugs to be found.

If this is incorrect, please file a bug on https://github.com/google/oss-fuzz/issues/new

Comment 3 by ClusterFuzz-External on Tue, Dec 8, 2020, 10:46 AM EST Project Member

Status: Verified (was: New)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5750916210491392 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_solidity&range=202012070615:202012080627

If this is incorrect, please file a bug on https://github.com/google/oss-fuzz/issues/new

Comment 4 by sheriffbot on Fri, Jan 8, 2021, 2:55 PM EST Project Member

Labels: -restrict-view-commit

This bug has been fixed for 30 days. It has been opened to the public.

- Your friendly Sheriffbot