Abrt · lldb_vs_lldb_eval_libfuzzer_test.cc

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State: `lldb_vs_lldb_eval_libfuzzer_test.cc`

Crash Type: Abrt
Created: Mon, Nov 15, 2021, 11:17 PM
Security: NO

Crash Address: 0x03e80001d69d
Sanitizer: address (ASAN)
Reliably Reproduces: YES

Issue: None
Platform: linux

Fuzzing Engine: libFuzzer
Fuzz Target: lldb_vs_lldb_eval_libfuzzer_test
Job Type: lldb-eval_libfuzzer_asan

Project: test-project

Fixed: NO

Minimized Testcase: (47 B) Unminimized Testcase: (47 B) Re-upload Testcase: Build:

LAST TESTED REVISION	REGRESSION REVISION RANGE
1:1 (No component revisions found!)	NA

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (48 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test -detect_leaks=0 -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-5281ac0f4ebf400b16b5d68af0ccc941da73dbfa
Time ran: 0.3964715003967285

INFO: found LLVMFuzzerCustomMutator (0x548640). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4167545821
INFO: Loaded 2 modules   (2040222 inline 8-bit counters): 1876506 [0x7f86b62f5520, 0x7f86b64bf73a), 163716 [0x1fe00a0, 0x2008024),
INFO: Loaded 2 PC tables (2040222 PCs): 1876506 [0x7f86b64bf740,0x7f86b81618e0), 163716 [0x2008028,0x2287868),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-5281ac0f4ebf400b16b5d68af0ccc941da73dbfa
[lldb-eval-fuzzer] expr: ns::CStyleEnum::V1 << (2.850722 ? true : sizeof *(&array33[!((ts).ch_field) % 3U]))
[lldb-eval-fuzzer]  cause: type mismatch
[lldb-eval-fuzzer]  lldb type     : unsigned int
[lldb-eval-fuzzer]  lldb-eval type: int
[lldb-eval-fuzzer] ================================================================================
AddressSanitizer:DEADLYSIGNAL
=================================================================
==168438==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000291f6 (pc 0x7f86a37e618b bp 0x7ffd964b30f0 sp 0x7ffd964b27d0 T0)
    #0 0x7f86a37e618b in raise
    #1 0x7f86a37c5858 in abort
    #2 0x549dbc in LLVMFuzzerTestOneInput /proc/self/cwd/tools/fuzzer/lldb_vs_lldb_eval_libfuzzer_test.cc:190:5
    #3 0x461293 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #4 0x44cd62 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #5 0x452815 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #6 0x47a4e2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #7 0x7f86a37c70b2 in __libc_start_main
    #8 0x42a38d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==168438==ABORTING


+-------------------------------------Release Build Unsymbolized Stacktrace (diff)-------------------------------------+

==================================================================
==168438==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000291f6 (pc 0x7f86a37e618b bp 0x7ffd964b30f0 sp 0x7ffd964b27d0 T0)
    #0 0x7f86a37e618b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7f86a37c5858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x549dbc  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x549dbc)
    #3 0x461293  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x461293)
    #4 0x44cd62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x44cd62)
    #5 0x452815  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x452815)
    #6 0x47a4e2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x47a4e2)
    #7 0x7f86a37c70b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x42a38d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x42a38d)
```

ORIGINAL STACKTRACE ON **REVISION 1** (49 LINES)

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test -detect_leaks=0 -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-5281ac0f4ebf400b16b5d68af0ccc941da73dbfa
Time ran: 0.39819812774658203

INFO: found LLVMFuzzerCustomMutator (0x548640). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 1632045475
INFO: Loaded 2 modules   (2040222 inline 8-bit counters): 1876506 [0x7f31f149e520, 0x7f31f166873a), 163716 [0x1fe00a0, 0x2008024),
INFO: Loaded 2 PC tables (2040222 PCs): 1876506 [0x7f31f1668740,0x7f31f330a8e0), 163716 [0x2008028,0x2287868),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-5281ac0f4ebf400b16b5d68af0ccc941da73dbfa
[lldb-eval-fuzzer] expr: ns::CStyleEnum::V1 << (2.850722 ? true : sizeof *(&array33[!((ts).ch_field) % 3U]))
[lldb-eval-fuzzer]  cause: type mismatch
[lldb-eval-fuzzer]  lldb type     : unsigned int
[lldb-eval-fuzzer]  lldb-eval type: int
[lldb-eval-fuzzer] ==================================================================
AddressSanitizer:DEADLYSIGNAL
=================================================================
==120477==ERROR: AddressSanitizer: ABRT on unknown address 0x03e80001d69d (pc 0x7f31de98f18b bp 0x7ffd1a174230 sp 0x7ffd1a173eb0 T0)
SCARINESS: 10 (signal)
    #0 0x7f31de98f18b in raise
    #1 0x7f31de96e858 in abort
    #2 0x549dbc in LLVMFuzzerTestOneInput /proc/self/cwd/tools/fuzzer/lldb_vs_lldb_eval_libfuzzer_test.cc:190:5
    #3 0x461293 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #4 0x44cd62 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #5 0x452815 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #6 0x47a4e2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #7 0x7f31de9700b2 in __libc_start_main
    #8 0x42a38d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==120477==ABORTING


+-------------------------------------Release Build Unsymbolized Stacktrace (diff)-------------------------------------+

==120477==ERROR: AddressSanitizer: ABRT on unknown address 0x03e80001d69d (pc 0x7f31de98f18b bp 0x7ffd1a174230 sp 0x7ffd1a173eb0 T0)
SCARINESS: 10 (signal)
    #0 0x7f31de98f18b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7f31de96e858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x549dbc  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x549dbc)
    #3 0x461293  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x461293)
    #4 0x44cd62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x44cd62)
    #5 0x452815  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x452815)
    #6 0x47a4e2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x47a4e2)
    #7 0x7f31de9700b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x42a38d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/lldb-eval_libfuzzer_asan/custom/lldb-eval/lldb_vs_lldb_eval_libfuzzer_test+0x42a38d)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-15 15:17:50 UTC] comput4-20211115-16:27: Fuzz task : Fuzzer libFuzzer_lldb_vs_lldb_eval_libfuzzer_test generated testcase crashed in 4 seconds (r1).
[2021-11-15 15:20:32 UTC] comput6-20211115-16:27: Minimize task started.
[2021-11-15 15:51:06 UTC] comput6-20211115-16:27: Minimize task errored out: LibFuzzer minimization failed.
[2021-11-22 03:10:42 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:43 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.