ASSERT · blst-blst-BLS_BatchVerify-(no algorithm)-difference

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State:
```
blst-blst-BLS_BatchVerify-(no algorithm)-difference
cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::abort
cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::compare
```

Crash Type: ASSERT
Created: Thu, Nov 18, 2021, 5:12 PM
Security: NO
Crash Address: ---
Sanitizer: address (ASAN)
Reliably Reproduces: YES
Issue: None
Platform: linux
Fuzzing Engine: libFuzzer
Fuzz Target: cryptofuzz-bls-signatures
Job Type: bls-signatures_libfuzzer_asan
Project: test-project
Fixed: NO

Minimized Testcase: (1 KB) Unminimized Testcase: (1 KB) Re-upload Testcase: Build:

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

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (64 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-a3470a69376d631bc6180dad48bb6e15a7d17b84
Time ran: 0.06429862976074219

INFO: found LLVMFuzzerCustomMutator (0xb7c270). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4188484491
INFO: Loaded 1 modules   (196070 inline 8-bit counters): 196070 [0x1f08818, 0x1f385fe),
INFO: Loaded 1 PC tables (196070 PCs): 196070 [0x1f38600,0x2236460),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-a3470a69376d631bc6180dad48bb6e15a7d17b84
Difference detected

Operation:

Module blst result:

true

Module blst result:

false

Assertion failure: blst-blst-BLS_BatchVerify-(no algorithm)-difference
AddressSanitizer:DEADLYSIGNAL
=================================================================
==170833==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029b51 (pc 0x7f6767efa18b bp 0x7ffd921cd170 sp 0x7ffd921cccf0 T0)
    #0 0x7f6767efa18b in raise
    #1 0x7f6767ed9858 in abort
    #2 0x7b6ca3 in cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::abort(std::__1::vector<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >, std::__1::allocator<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > >, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >) const /src/cryptofuzz/executor.cpp:1944:5
    #3 0x7b4eca in cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::compare(std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::BLS_BatchVerify>, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::BLS_BatchVerify> > > const&, std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<bool> >, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<bool> > > > const&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:1923:13
    #4 0x7bcc69 in cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2182:9
    #5 0x59f7df in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:279:41
    #6 0xa32d1d in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #7 0x495cd3 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x481582 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x487035 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x4afd32 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7f6767edb0b2 in __libc_start_main
    #12 0x45e81d in _start
```

```
42
43 AddressSanitizer can not provide additional info.
44 SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
45 ==170833==ABORTING
46
47
48 +--------------------------------------Release Build Unsymbolized Stacktrace (diff)--------------------------------------+
49
50 ================================================================
51 ==170833==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029b51 (pc 0x7f6767efa18b bp 0x7ffd921cd170 sp 0x7ffd921cccf0 T0)
52     #0 0x7f6767efa18b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
53     #1 0x7f6767ed9858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
54     #2 0x7b6ca3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x7b6ca
   3)
55     #3 0x7b4eca  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x7b4ec
   a)
56     #4 0x7bcc69  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x7bcc6
   9)
57     #5 0x59f7df  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x59f7d
   f)
58     #6 0xa32d1d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0xa32d1
   d)
59     #7 0x495cd3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x495cd
   3)
60     #8 0x481582  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x48158
   2)
61     #9 0x487035  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x48703
   5)
62     #10 0x4afd32  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x4afd3
   2)
63     #11 0x7f6767edb0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
64     #12 0x45e81d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x45e81
   d)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (64 LINES) ---

```
1 [Environment] ASAN_OPTIONS=exitcode=77
2 +--------------------------------------Release Build Stacktrace--------------------------------------+
3 Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures -rss_limit_mb=256
  0 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/e205d9b18f14c4a061ef775b10292ff4376d631bc6180dad48bb6e15a7d17b8
  4
4 Time ran: 0.05737781524658203
5
6 INFO: found LLVMFuzzerCustomMutator (0xb7c270). Disabling -len_control by default.
7 INFO: Running with entropic power schedule (0xFF, 100).
8 INFO: Seed: 4123109869
9 INFO: Loaded 1 modules   (196070 inline 8-bit counters): 196070 [0x1f08818, 0x1f385fe),
10 INFO: Loaded 1 PC tables (196070 PCs): 196070 [0x1f38600,0x2236460),
11 /clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures: Running 1 inputs 100 time
   (s) each.
12 Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/e205d9b18f14c4a061ef775b10292ff4376d631bc6180dad48bb6e15a7d17b84
13 Difference detected
14
15 Operation:
16
17 Module blst result:
18
19 true
20
21 Module blst result:
22
23 false
24
25 Assertion failure: blst-blst-BLS_BatchVerify-(no algorithm)-difference
26 AddressSanitizer:DEADLYSIGNAL
27 ================================================================
28 ==35853==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800008c0d (pc 0x7fc50ff5618b bp 0x7ffc83b7ca70 sp 0x7ffc83b7c5f0 T0)
29     #0 0x7fc50ff5618b in raise
30     #1 0x7fc50ff35858 in abort
31     #2 0x7b6ca3 in cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::abort(std::__1::vector<std::__1::basic_string<char, std::
   __1::char_traits<char>, std::__1::allocator<char> >, std::__1::allocator<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocat
   or<char> > > >, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >, std::__1::basic_string<char, std::__1::char_t
   raits<char>, std::__1::allocator<char> >, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >) const /src/cryptofu
   zz/executor.cpp:1944:5
32     #3 0x7b4eca in cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::compare(std::__1::vector<std::__1::pair<std::__1::shared_
   ptr<cryptofuzz::Module>, cryptofuzz::operation::BLS_BatchVerify>, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, crypt
   ofuzz::operation::BLS_BatchVerify> > > const&, std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<bool> >,
   std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<bool> > > > const&, unsigned char const*, unsigned l
   ong) const /src/cryptofuzz/executor.cpp:1923:13
33     #4 0x7bcc69 in cryptofuzz::ExecutorBase<bool, cryptofuzz::operation::BLS_BatchVerify>::Run(fuzzing::datasource::Datasource&, unsigned char const
```

```
*, unsigned long) const /src/cryptofuzz/executor.cpp:2182:9
    #5 0x59f7df in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:279:41
    #6 0xa32d1d in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #7 0x495cd3 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x481582 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x487035 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x4afd32 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7fc50ff370b2 in __libc_start_main
    #12 0x45e81d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==35853==ABORTING


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

================================================================
==35853==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800008c0d (pc 0x7fc50ff5618b bp 0x7ffc83b7ca70 sp 0x7ffc83b7c5f0 T0)
    #0 0x7fc50ff5618b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7fc50ff35858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x7b6ca3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x7b6ca3)
    #3 0x7b4eca  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x7b4eca)
    #4 0x7bcc69  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x7bcc69)
    #5 0x59f7df  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x59f7df)
    #6 0xa32d1d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0xa32d1d)
    #7 0x495cd3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x495cd3)
    #8 0x481582  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x481582)
    #9 0x487035  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x487035)
    #10 0x4afd32  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x4afd32)
    #11 0x7fc50ff370b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x45e81d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/bls-signatures_libfuzzer_asan/custom/bls-signatures/cryptofuzz-bls-signatures+0x45e81d)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-18 09:12:08 UTC] comput13-20211115-16:27: Fuzz task : Fuzzer libFuzzer_cryptofuzz-bls-signatures generated testcase crashed in 5483 seconds (r1).
[2021-11-18 09:15:59 UTC] comput3-20211115-16:27: Minimize task started.
[2021-11-18 09:41:16 UTC] comput3-20211115-16:27: Minimize task finished.
[2021-11-22 03:11:04 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:11:04 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.