Abrt · cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Sig...

Loaded 3 minutes ago

REDO TASK DELETE

OVERVIEW

Crash State:
```
cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Signature, cryptofuzz::ope
cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Signature, cryptofuzz::ope
cryptofuzz::Driver::Run
```

Crash Type: Abrt
Created: Tue, Nov 16, 2021, 11:31 PM
Security: NO
Crash Address: 0x03e8000100f0
Sanitizer: address (ASAN)
Reliably Reproduces: YES
Issue: None
Platform: linux
Fuzzing Engine: libFuzzer
Fuzz Target: cryptofuzz-openssl
Job Type: cryptofuzz_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 (50 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-ac46d2dbc82a67535a61253231f644715f548a82
Time ran: 0.05210614204406738

INFO: found LLVMFuzzerCustomMutator (0xa8e530). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4179012323
INFO: Loaded 1 modules   (348730 inline 8-bit counters): 348730 [0x38b0910, 0x3905b4a),
INFO: Loaded 1 PC tables (348730 PCs): 348730 [0x3905b50,0x3e57ef0),
INFO: 65536 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-ac46d2dbc82a67535a61253231f644715f548a82
AddressSanitizer:DEADLYSIGNAL
=================================================================
==169700==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000296e4 (pc 0x7fe0df15818b bp 0x7ffce53cfc70 sp 0x7ffce53cf490 T0)
    #0 0x7fe0df15818b in raise
    #1 0x7fe0df137858 in abort
    #2 0x664b03 in cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Signature, cryptofuzz::operation::ECDSA_Sign>::postprocess(std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::ECDSA_Sign&, std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::component::ECDSA_Signature> > const&) const /src/cryptofuzz/executor.cpp:498:13
    #3 0x661d06 in cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Signature, cryptofuzz::operation::ECDSA_Sign>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2178:9
    #4 0x5a42c0 in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:171:36
    #5 0x95ff3d in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #6 0x4990b3 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #7 0x4849c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #8 0x48a48a in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #9 0x4b33b2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #10 0x7fe0df1390b2 in __libc_start_main
    #11 0x461c4d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==169700==ABORTING


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

=================================================================
==169700==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000296e4 (pc 0x7fe0df15818b bp 0x7ffce53cfc70 sp 0x7ffce53cf490 T0)
    #0 0x7fe0df15818b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7fe0df137858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x664b03  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x664b03)
    #3 0x661d06  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x661d06)
    #4 0x5a42c0  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x5a42c0)
    #5 0x95ff3d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x95ff3d)
    #6 0x4990b3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x4990b3)
    #7 0x4849c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x4849c2)
```

```
    #8 0x48a48a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x48a48a)
    #9 0x4b33b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x4b33b2)
    #10 0x7fe0df1390b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #11 0x461c4d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x461c4d)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (50 LINES) ---

```
[Environment] ASAN_OPTIONS=dedup_token_length=3:exitcode=77:symbolize=1
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/7386162fb604944a58d89802c318d30dc82a67535a61253231f644715f548a82
Time ran: 0.04616665840148926

INFO: found LLVMFuzzerCustomMutator (0xa8e530). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 513038197
INFO: Loaded 1 modules   (348730 inline 8-bit counters): 348730 [0x38b0910, 0x3905b4a),
INFO: Loaded 1 PC tables (348730 PCs): 348730 [0x3905b50,0x3e57ef0),
INFO: 65536 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/7386162fb604944a58d89802c318d30dc82a67535a61253231f644715f548a82
AddressSanitizer:DEADLYSIGNAL
=================================================================
==65776==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000100f0 (pc 0x7fea3457318b bp 0x7ffd8ba51950 sp 0x7ffd8ba51170 T0)
    #0 0x7fea3457318b in raise
    #1 0x7fea34552858 in abort
    #2 0x664b03 in cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Signature, cryptofuzz::operation::ECDSA_Sign>::postprocess(std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::ECDSA_Sign&, std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::component::ECDSA_Signature> > const&) const /src/cryptofuzz/executor.cpp:498:13
    #3 0x661d06 in cryptofuzz::ExecutorBase<cryptofuzz::component::ECDSA_Signature, cryptofuzz::operation::ECDSA_Sign>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2178:9
    #4 0x5a42c0 in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:171:36
    #5 0x95ff3d in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #6 0x4990b3 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #7 0x4849c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #8 0x48a48a in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #9 0x4b33b2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #10 0x7fea345540b2 in __libc_start_main
    #11 0x461c4d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==65776==ABORTING


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

=================================================================
==65776==ERROR: AddressSanitizer: ABRT on unknown address 0x03e8000100f0 (pc 0x7fea3457318b bp 0x7ffd8ba51950 sp 0x7ffd8ba51170 T0)
    #0 0x7fea3457318b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7fea34552858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x664b03  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x664b03)
    #3 0x661d06  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x661d06)
    #4 0x5a42c0  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x5a42c0)
    #5 0x95ff3d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x95ff3d)
    #6 0x4990b3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x4990b3)
    #7 0x4849c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x4849c2)
    #8 0x48a48a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x48a48a)
    #9 0x4b33b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x4b33b2)
    #10 0x7fea345540b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #11 0x461c4d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-openssl+0x461c4d)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-16 15:31:40 UTC] comput19-20211115-16:27: Fuzz task : Fuzzer libFuzzer_cryptofuzz-openssl generated testcase crashed in 375 seconds (r1).
[2021-11-16 15:36:13 UTC] comput17-20211115-16:27: Minimize task started.
[2021-11-16 16:14:01 UTC] comput17-20211115-16:27: Minimize task finished.
[2021-11-22 03:10:54 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:55 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.