ASSERT · noble-secp256k1-trezor-firmware-ECC_Point_Mul-(no algorit...

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State: noble-secp256k1-trezor-firmware-ECC_Point_Mul-(no algorithm)-difference
cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operatio
cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operatio

Crash Type: ASSERT Created: Mon, Nov 15, 2021, 11:20 PM Security: NO

Crash Address: --- Sanitizer: address (ASAN) Reliably Reproduces: YES

Issue: None Platform: linux

Fuzzing Engine: libFuzzer Fuzz Target: cryptofuzz-boringssl-noasm Job Type: cryptofuzz_libfuzzer_asan

Project: test-project

Related: Group 254

Fixed: NO

Minimized Testcase: (537 B) Unminimized Testcase: (874 B) Re-upload Testcase: Build:

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

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (74 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-382d3510c04669cdcaf1f0a0d115930e48a2cc03
Time ran: 0.1583418846130371

INFO: found LLVMFuzzerCustomMutator (0xa8f020). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4169984252
INFO: Loaded 1 modules   (336529 inline 8-bit counters): 336529 [0x3650a10, 0x36a2ca1),
INFO: Loaded 1 PC tables (336529 PCs): 336529 [0x36a2ca8,0x3bc55b8),
INFO: 65536 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-382d3510c04669cdcaf1f0a0d115930e48a2cc03
Difference detected

Operation:
operation name: ECC_Point_Mul
ecc curve: secp256k1
A X: 2099722
A Y: 431964587762171763199047270187455665383154135036494166507
B: 76884956397045344220809746629001649093037950200943055203735601445031516197748

Module noble-secp256k1 result:

X: 113378631514367647047444983903855111860357459299363675073133611552356088368449
Y: 22618537924462869714036999851335165639159392587359165150069581876333737435097


Module trezor-firmware result:

X: 51001657859126333878497609847758655036986015646520436018124368662690013122475
Y: 113913346734835111914948561522452891000972583019799131854878002731583666386945


Assertion failure: noble-secp256k1-trezor-firmware-ECC_Point_Mul-(no algorithm)-difference
AddressSanitizer:DEADLYSIGNAL
=================================================================
==168712==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029308 (pc 0x7f38b129b18b bp 0x7ffc3550a530 sp 0x7ffc3550a210 T0)
    #0 0x7f38b129b18b in raise
    #1 0x7f38b127a858 in abort
    #2 0x6d73a4 in cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operation::ECC_Point_Mul>::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 0x6d5699 in cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operation::ECC_Point_Mul>::compare(std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::ECC_Point_Mul>, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<c
ryptofuzz::Module>, cryptofuzz::operation::ECC_Point_Mul> > > const&, std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::component::BignumPair> >, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::component::BignumPair> > > > const&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:1923:13
    #4 0x6db9bc in cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operation::ECC_Point_Mul>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2182:9
    #5 0x5a4f56 in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:210:39
    #6 0x9608ed in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #7 0x4998a3 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x4851b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x48ac7a in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x4b3ba2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7f38b127c0b2 in __libc_start_main
    #12 0x46243d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==168712==ABORTING


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

=================================================================
==168712==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029308 (pc 0x7f38b129b18b bp 0x7ffc3550a530 sp 0x7ffc3550a210 T0)
    #0 0x7f38b129b18b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7f38b127a858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x6d73a4  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x6d73a4)
    #3 0x6d5699  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x6d5699)
    #4 0x6db9bc  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x6db9bc)
    #5 0x5a4f56  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x5a4f56)
    #6 0x9608ed  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x9608ed)
    #7 0x4998a3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x4998a3)
    #8 0x4851b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x4851b2)
    #9 0x48ac7a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x48ac7a)
    #10 0x4b3ba2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x4b3ba2)
    #11 0x7f38b127c0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x46243d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x46243d)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (74 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-boringssl-noasm -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/bbfaaadec6bff4ea161a4420409b6a0ec04669cdcaf1f0a0d115930e48a2cc03
Time ran: 0.15223050117492676

INFO: found LLVMFuzzerCustomMutator (0xa8f020). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 1614492725
INFO: Loaded 1 modules   (336529 inline 8-bit counters): 336529 [0x3650a10, 0x36a2ca1),
INFO: Loaded 1 PC tables (336529 PCs): 336529 [0x36a2ca8,0x3bc55b8),
INFO: 65536 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/bbfaaadec6bff4ea161a4420409b6a0ec04669cdcaf1f0a0d115930e48a2cc03
Difference detected

Operation:
operation name: ECC_Point_Mul
ecc curve: secp256k1
A X: 2099722
A Y: 431964587762171763199047270187455665383154135036494166507
B: 76884956397045344220809746629001649093037950200943055203735601445031516197748

Module noble-secp256k1 result:

X: 113378631514367647047444983903855111860357459299363675073133611552356088368449
Y: 22618537924462869714036999851335165639159392587359165150069581876333737435097


Module trezor-firmware result:

X: 51001657859126333878497609847758655036986015646520436018124368662690013122475
Y: 113913346734835111914948561522452891000972583019799131854878002731583666386945


Assertion failure: noble-secp256k1-trezor-firmware-ECC_Point_Mul-(no algorithm)-difference
```

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==133810==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800020ab2 (pc 0x7f16897a918b bp 0x7ffe0c490530 sp 0x7ffe0c490210 T0)
    #0 0x7f16897a918b in raise
    #1 0x7f1689788858 in abort
    #2 0x6d73a4 in cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operation::ECC_Point_Mul>::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 0x6d5699 in cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operation::ECC_Point_Mul>::compare(std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::ECC_Point_Mul>, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::ECC_Point_Mul> > > const&, std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::component::BignumPair> >, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::component::BignumPair> > > > const&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:1923:13
    #4 0x6db9bc in cryptofuzz::ExecutorBase<cryptofuzz::component::BignumPair, cryptofuzz::operation::ECC_Point_Mul>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2182:9
    #5 0x5a4f56 in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:210:39
    #6 0x9608ed in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #7 0x4998a3 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x4851b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x48ac7a in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x4b3ba2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7f168978a0b2 in __libc_start_main
    #12 0x46243d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==133810==ABORTING


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

=================================================================
==133810==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800020ab2 (pc 0x7f16897a918b bp 0x7ffe0c490530 sp 0x7ffe0c490210 T0)
    #0 0x7f16897a918b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7f1689788858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x6d73a4  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x6d73a4)
    #3 0x6d5699  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x6d5699)
    #4 0x6db9bc  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x6db9bc)
    #5 0x5a4f56  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x5a4f56)
    #6 0x9608ed  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x9608ed)
    #7 0x4998a3  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x4998a3)
    #8 0x4851b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x4851b2)
    #9 0x48ac7a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x48ac7a)
    #10 0x4b3ba2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x4b3ba2)
    #11 0x7f168978a0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x46243d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-boringssl-noasm+0x46243d)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

```
[2021-11-15 15:20:30 UTC] comput6-20211115-16:27: Fuzz task : Fuzzer libFuzzer_cryptofuzz-boringssl-noasm generated testcase crashed in 232 seconds (r1).
[2021-11-15 15:51:07 UTC] comput6-20211115-16:27: Minimize task started.
[2021-11-15 16:34:00 UTC] comput6-20211115-16:27: Minimize task finished.
[2021-11-22 03:10:45 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:46 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.
```