ASSERT · OpenSSL-mbed TLS-CMAC-(no algorithm)-difference

Loaded 2 minutes ago

REDO TASK DELETE

OVERVIEW

Crash State:
```
OpenSSL-mbed TLS-CMAC-(no algorithm)-difference
cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::abort
cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::compa
```

Crash Type: ASSERT
Created: Wed, Nov 17, 2021, 3:37 AM
Security: NO

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

Issue: None
Platform: linux

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

Project: test-project

Related: Group 632

Fixed: **NO**

Minimized Testcase: (758 B) 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 (75 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-ff25d4be6a794237f6f1e63e0b1eed26054255e5
Time ran: 0.044087886810302734

INFO: found LLVMFuzzerCustomMutator (0xa8dfe0). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4182302385
INFO: Loaded 1 modules   (353203 inline 8-bit counters): 353203 [0x385ba10, 0x38b1dc3),
INFO: Loaded 1 PC tables (353203 PCs): 353203 [0x38b1dc8,0x3e158f8),
INFO: 65536 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-ff25d4be6a794237f6f1e63e0b1eed26054255e5
Difference detected

Operation:
operation name: CMAC
cipher iv: {0xe1, 0x42, 0x0b, 0xce, 0x98, 0x49, 0x07, 0x8b, 0x89, 0x14, 0xf4, 0x19, 0xc5, 0x0c, 0xff, 0xff,
 0xb9, 0x75, 0x3a, 0x3e, 0x46, 0xdb, 0xd7, 0xa4, 0xa6, 0x98, 0x01, 0x73, 0xfd, 0x94, 0x59, 0x12,
 0x79, 0xb0, 0x81, 0xe2, 0x3a, 0xd3, 0x27, 0x50, 0x6a, 0xe5, 0xe7, 0xc1, 0x2c, 0xcb, 0x72, 0x95,
 0xa3, 0x69, 0x67, 0x38, 0xfe, 0xaa, 0x6d, 0x10, 0x5b, 0x6f, 0x28, 0x7e, 0xe2, 0xa1, 0x45, 0xee} (64 bytes)
cipher key: {0x65, 0xc1, 0x0b, 0xe4, 0x2e, 0x61, 0xf6, 0xbe, 0x45, 0x31, 0xa4, 0x9d, 0x54, 0x99, 0x3e, 0x68} (16 bytes)
cipher: AES_128_ECB
cleartext: {0xfe, 0x86, 0x1e, 0x50, 0xd5, 0x11, 0x54, 0x4d, 0x6e, 0x3d, 0xba, 0xc1, 0x6d, 0x6f, 0x78, 0x90,
 0x76, 0x12, 0xb7, 0x9c, 0x31, 0x82, 0x98, 0xd0, 0x46, 0x30, 0x46, 0x0f} (28 bytes)
key: {0x65, 0xc1, 0x0b, 0xe4, 0x2e, 0x61, 0xf6, 0xbe, 0x45, 0x31, 0xa4, 0x9d, 0x54, 0x99, 0x3e, 0x68} (16 bytes)

Module OpenSSL result:

{0x63, 0x6b, 0x45, 0x70, 0xbf, 0xaa, 0x8b, 0xc1, 0x70, 0xf9, 0xe6, 0xd8, 0x5d, 0xa0, 0xd2, 0xef} (16 bytes)

Module mbed TLS result:

{0xa0, 0x44, 0x98, 0x4e, 0x94, 0xd0, 0xc1, 0xd4, 0x7f, 0x2e, 0xb2, 0xfb, 0xe8, 0xf4, 0x83, 0x1e} (16 bytes)

Assertion failure: OpenSSL-mbed TLS-CMAC-(no algorithm)-difference
AddressSanitizer:DEADLYSIGNAL
=================================================================
==170069==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029855 (pc 0x7f01a70c318b bp 0x7ffc7bbd3c90 sp 0x7ffc7bbd3970 T0)
    #0 0x7f01a70c318b in raise
    #1 0x7f01a70a2858 in abort
    #2 0x5c1944 in cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::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 0x5bfbd1 in cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::compare(std::__1::vector<std::__1::pair<std::__1::shar
ed_ptr<cryptofuzz::Module>, cryptofuzz::operation::CMAC>, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::CMAC> > > const&, std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::Buffer> >, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::Buffer> > > > const&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:1923:13
    #4 0x5c5d37 in cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2182:9
    #5 0x5a3773 in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:120:30
    #6 0x95f8ad in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #7 0x498863 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x484172 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x489c3a in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x4b2b62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7f01a70a40b2 in __libc_start_main
    #12 0x4613fd in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==170069==ABORTING


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

=================================================================
==170069==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800029855 (pc 0x7f01a70c318b bp 0x7ffc7bbd3c90 sp 0x7ffc7bbd3970 T0)
    #0 0x7f01a70c318b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7f01a70a2858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x5c1944  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5c1944)
    #3 0x5bfbd1  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5bfbd1)
    #4 0x5c5d37  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5c5d37)
    #5 0x5a3773  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5a3773)
    #6 0x95f8ad  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x95f8ad)
    #7 0x498863  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x498863)
    #8 0x484172  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x484172)
    #9 0x489c3a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x489c3a)
    #10 0x4b2b62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x4b2b62)
    #11 0x7f01a70a40b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x4613fd  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x4613fd)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (75 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-libressl-noasm -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/e4ec5f9dc08d49b87e07634682eaa5d76a794237f6f1e63e0b1eed26054255e5
Time ran: 0.035398244857788086

INFO: found LLVMFuzzerCustomMutator (0xa8dfe0). Disabling -len_control by default.
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 1324554968
INFO: Loaded 1 modules   (353203 inline 8-bit counters): 353203 [0x385ba10, 0x38b1dc3),
INFO: Loaded 1 PC tables (353203 PCs): 353203 [0x38b1dc8,0x3e158f8),
INFO: 65536 Extra Counters
/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/e4ec5f9dc08d49b87e07634682eaa5d76a794237f6f1e63e0b1eed26054255e5
Difference detected

Operation:
operation name: CMAC
cipher iv: {0xe1, 0x42, 0x0b, 0xce, 0x98, 0x49, 0x07, 0x8b, 0x89, 0x14, 0xf4, 0x19, 0xc5, 0x0c, 0xff, 0xff,
 0xb9, 0x75, 0x3a, 0x3e, 0x46, 0xdb, 0xd7, 0xa4, 0xa6, 0x98, 0x01, 0x73, 0xfd, 0x94, 0x59, 0x12,
 0x79, 0xb0, 0x81, 0xe2, 0x3a, 0xd3, 0x27, 0x50, 0x6a, 0xe5, 0xe7, 0xc1, 0x2c, 0xcb, 0x72, 0x95,
 0xa3, 0x69, 0x67, 0x38, 0xfe, 0xaa, 0x6d, 0x10, 0x5b, 0x6f, 0x28, 0x7e, 0xe2, 0xa1, 0x45, 0xee} (64 bytes)
cipher key: {0x65, 0xc1, 0x0b, 0xe4, 0x2e, 0x61, 0xf6, 0xbe, 0x45, 0x31, 0xa4, 0x9d, 0x54, 0x99, 0x3e, 0x68} (16 bytes)
cipher: AES_128_ECB
cleartext: {0xfe, 0x86, 0x1e, 0x50, 0xd5, 0x11, 0x54, 0x4d, 0x6e, 0x3d, 0xba, 0xc1, 0x6d, 0x6f, 0x78, 0x90,
 0x76, 0x12, 0xb7, 0x9c, 0x31, 0x82, 0x98, 0xd0, 0x46, 0x30, 0x46, 0x0f} (28 bytes)
key: {0x65, 0xc1, 0x0b, 0xe4, 0x2e, 0x61, 0xf6, 0xbe, 0x45, 0x31, 0xa4, 0x9d, 0x54, 0x99, 0x3e, 0x68} (16 bytes)

Module OpenSSL result:

{0x63, 0x6b, 0x45, 0x70, 0xbf, 0xaa, 0x8b, 0xc1, 0x70, 0xf9, 0xe6, 0xd8, 0x5d, 0xa0, 0xd2, 0xef} (16 bytes)

Module mbed TLS result:

{0xa0, 0x44, 0x98, 0x4e, 0x94, 0xd0, 0xc1, 0xd4, 0x7f, 0x2e, 0xb2, 0xfb, 0xe8, 0xf4, 0x83, 0x1e} (16 bytes)
```

```

Assertion failure: OpenSSL-mbed TLS-CMAC-(no algorithm)-difference
AddressSanitizer:DEADLYSIGNAL
=================================================================
==105928==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800019dc8 (pc 0x7f016dfa918b bp 0x7ffe689cd2b0 sp 0x7ffe689ccf90 T0)
    #0 0x7f016dfa918b in raise
    #1 0x7f016df88858 in abort
    #2 0x5c1944 in cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::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 0x5bfbd1 in cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::compare(std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::CMAC>, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, cryptofuzz::operation::CMAC> > > const&, std::__1::vector<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::Buffer> >, std::__1::allocator<std::__1::pair<std::__1::shared_ptr<cryptofuzz::Module>, std::__1::optional<cryptofuzz::Buffer> > > > const&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:1923:13
    #4 0x5c5d37 in cryptofuzz::ExecutorBase<cryptofuzz::Buffer, cryptofuzz::operation::CMAC>::Run(fuzzing::datasource::Datasource&, unsigned char const*, unsigned long) const /src/cryptofuzz/executor.cpp:2182:9
    #5 0x5a3773 in cryptofuzz::Driver::Run(unsigned char const*, unsigned long) const /src/cryptofuzz/driver.cpp:120:30
    #6 0x95f8ad in LLVMFuzzerTestOneInput /src/cryptofuzz/entry.cpp:587:13
    #7 0x498863 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x484172 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x489c3a in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x4b2b62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7f016df8a0b2 in __libc_start_main
    #12 0x4613fd in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: ABRT (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
==105928==ABORTING


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

=================================================================
==105928==ERROR: AddressSanitizer: ABRT on unknown address 0x03e800019dc8 (pc 0x7f016dfa918b bp 0x7ffe689cd2b0 sp 0x7ffe689ccf90 T0)
    #0 0x7f016dfa918b  (/lib/x86_64-linux-gnu/libc.so.6+0x4618b)
    #1 0x7f016df88858  (/lib/x86_64-linux-gnu/libc.so.6+0x25858)
    #2 0x5c1944  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5c1944)
    #3 0x5bfbd1  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5bfbd1)
    #4 0x5c5d37  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5c5d37)
    #5 0x5a3773  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x5a3773)
    #6 0x95f8ad  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x95f8ad)
    #7 0x498863  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x498863)
    #8 0x484172  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x484172)
    #9 0x489c3a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x489c3a)
    #10 0x4b2b62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x4b2b62)
    #11 0x7f016df8a0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x4613fd  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/cryptofuzz_libfuzzer_asan/custom/cryptofuzz/cryptofuzz-libressl-noasm+0x4613fd)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-16 19:37:30 UTC] comput16-20211115-16:27: Fuzz task : Fuzzer libFuzzer_cryptofuzz-libressl-noasm generated testcase crashed in 57 seconds (r1).
[2021-11-16 19:39:02 UTC] comput16-20211115-16:27: Minimize task started.
[2021-11-16 20:21:53 UTC] comput16-20211115-16:27: Minimize task finished.
[2021-11-22 03:10:57 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:58 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.