Null-dereference READ · blosc2_stdio_seek

Loaded 3 minutes ago

REDO TASK DELETE

OVERVIEW

Crash State:
```
blosc2_stdio_seek
blosc_d
do_job
```

Crash Type: Null-dereference READ
Created: Tue, Nov 16, 2021, 5:25 AM
Security: NO
Crash Address: 0x000000000000
Sanitizer: address (ASAN)
Reliably Reproduces: YES
Issue: None
Platform: linux
Fuzzing Engine: libFuzzer
Fuzz Target: decompress_frame_fuzzer
Job Type: c-blosc2_libfuzzer_asan
Project: test-project
Fixed: NO

Minimized Testcase: (23 KB) Unminimized Testcase: (23 KB) Re-upload Testcase: Build:

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

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (55 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-dc06e7857f98c5402c9e02c938056987e49eaef6
Time ran: 0.02154064178466797

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4172538042
INFO: Loaded 1 modules   (53184 inline 8-bit counters): 53184 [0xd10d20, 0xd1dce0),
INFO: Loaded 1 PC tables (53184 PCs): 53184 [0xbe6840,0xcb6440),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-dc06e7857f98c5402c9e02c938056987e49eaef6
AddressSanitizer:DEADLYSIGNAL
=================================================================
==168957==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005c9b1c bp 0x7ffd67efbf50 sp 0x7ffd67efbf50 T0)
==168957==The signal is caused by a READ memory access.
==168957==Hint: address points to the zero page.
    #0 0x5c9b1c in blosc2_stdio_seek /src/c-blosc2/blosc/blosc2-stdio.c:47:21
    #1 0x573ba5 in blosc_d /src/c-blosc2/blosc/blosc2.c:1440:7
    #2 0x566467 in serial_blosc /src/c-blosc2/blosc/blosc2.c:1736:16
    #3 0x566467 in do_job /src/c-blosc2/blosc/blosc2.c:1901:15
    #4 0x56d58c in blosc_run_decompression_with_context /src/c-blosc2/blosc/blosc2.c:2541:13
    #5 0x56d9dc in blosc2_decompress_ctx /src/c-blosc2/blosc/blosc2.c:2561:12
    #6 0x5b5121 in frame_decompress_chunk /src/c-blosc2/blosc/frame.c:3377:24
    #7 0x58f2c6 in blosc2_schunk_decompress_chunk /src/c-blosc2/blosc/schunk.c:991:17
    #8 0x55dba6 in LLVMFuzzerTestOneInput /src/c-blosc2/tests/fuzz/fuzz_decompress_frame.c:37:15
    #9 0x456c03 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #10 0x4424b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #11 0x447f65 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #12 0x470c62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #13 0x7f2929db80b2 in __libc_start_main
    #14 0x41f74d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x5c9b1c)
==168957==ABORTING


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

==168957==The signal is caused by a READ memory access.
==168957==Hint: address points to the zero page.
    #0 0x5c9b1c  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x5c9b1c)
    #1 0x573ba5  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x573ba5)
    #2 0x566467  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x566467)
    #3 0x56d58c  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x56d58c)
    #4 0x56d9dc  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x56d9dc)
    #5 0x5b5121  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x5b5121)
```

```
    #6 0x58f2c6  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x58f2c6)
    #7 0x55dba6  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x55dba6)
    #8 0x456c03  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x456c03)
    #9 0x4424b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x4424b2)
    #10 0x447f65  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x447f65)
    #11 0x470c62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x470c62)
    #12 0x7f2929db80b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #13 0x41f74d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x41f74d)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (55 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/bfaf138bb2b1353008e696144dc2a5237f98c5402c9e02c938056987e49eaef6
Time ran: 0.015801668167114258

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 261685717
INFO: Loaded 1 modules   (53184 inline 8-bit counters): 53184 [0xd10d20, 0xd1dce0),
INFO: Loaded 1 PC tables (53184 PCs): 53184 [0xbe6840,0xcb6440),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/bfaf138bb2b1353008e696144dc2a5237f98c5402c9e02c938056987e49eaef6
AddressSanitizer:DEADLYSIGNAL
=================================================================
==92893==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005c9b1c bp 0x7ffc0b8ce610 sp 0x7ffc0b8ce610 T0)
==92893==The signal is caused by a READ memory access.
==92893==Hint: address points to the zero page.
    #0 0x5c9b1c in blosc2_stdio_seek /src/c-blosc2/blosc/blosc2-stdio.c:47:21
    #1 0x573ba5 in blosc_d /src/c-blosc2/blosc/blosc2.c:1440:7
    #2 0x566467 in serial_blosc /src/c-blosc2/blosc/blosc2.c:1736:16
    #3 0x566467 in do_job /src/c-blosc2/blosc/blosc2.c:1901:15
    #4 0x56d58c in blosc_run_decompression_with_context /src/c-blosc2/blosc/blosc2.c:2541:13
    #5 0x56d9dc in blosc2_decompress_ctx /src/c-blosc2/blosc/blosc2.c:2561:12
    #6 0x5b5121 in frame_decompress_chunk /src/c-blosc2/blosc/frame.c:3377:24
    #7 0x58f2c6 in blosc2_schunk_decompress_chunk /src/c-blosc2/blosc/schunk.c:991:17
    #8 0x55dba6 in LLVMFuzzerTestOneInput /src/c-blosc2/tests/fuzz/fuzz_decompress_frame.c:37:15
    #9 0x456c03 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #10 0x4424b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #11 0x447f65 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #12 0x470c62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #13 0x7f74c6a5d0b2 in __libc_start_main
    #14 0x41f74d in _start

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x5c9b1c)
==92893==ABORTING


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

==92893==The signal is caused by a READ memory access.
==92893==Hint: address points to the zero page.
    #0 0x5c9b1c  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x5c9b1c)
    #1 0x573ba5  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x573ba5)
    #2 0x566467  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x566467)
    #3 0x56d58c  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x56d58c)
    #4 0x56d9dc  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x56d9dc)
    #5 0x5b5121  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x5b5121)
    #6 0x58f2c6  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x58f2c6)
    #7 0x55dba6  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x55dba6)
    #8 0x456c03  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x456c03)
    #9 0x4424b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x4424b2)
    #10 0x447f65  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x447f65)
    #11 0x470c62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x470c62)
    #12 0x7f74c6a5d0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #13 0x41f74d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_frame_fuzzer+0x41f74d)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-15 21:25:38 UTC] comput6-20211115-16:27: Fuzz task : Fuzzer libFuzzer_decompress_frame_fuzzer generated testcase crashed in 0 seconds (r1).
[2021-11-15 21:43:21 UTC] comput4-20211115-16:27: Minimize task started.
[2021-11-15 22:09:21 UTC] comput4-20211115-16:27: Minimize task finished.

[2021-11-22 03:10:48 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:48 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.