Heap-buffer-overflow READ 4 · ndlz8_decompress

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State: ndlz8_decompress
blosc_d
do_job

Crash Type: Heap-buffer-overflow READ 4

Created: Wed, Nov 17, 2021, 10:09 PM

Security: **YES (Medium)**

Crash Address: 0x6040000000c0

Sanitizer: address (ASAN)

Reliably Reproduces: YES

Issue: None

Platform: linux

Fuzzing Engine: libFuzzer

Fuzz Target: decompress_chunk_fuzzer

Job Type: c-blosc2_libfuzzer_asan

Project: test-project

Related: Group 790

Fixed: NO

Minimized Testcase: (48 B) Unminimized Testcase: (48 B) Re-upload Testcase: Build:

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

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (97 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-9f1cc8a1f781b603b60a40d07c75fada3aff7d71
Time ran: 0.020229101181030273

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4187480574
INFO: Loaded 1 modules   (53183 inline 8-bit counters): 53183 [0xd10cc0, 0xd1dc7f),
INFO: Loaded 1 PC tables (53183 PCs): 53183 [0xbe67c0,0xcb63b0),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-9f1cc8a1f781b603b60a40d07c75fada3aff7d71
=================================================================
==170707==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000000c0 at pc 0x000000abd8c5 bp 0x7ffef4de0170 sp 0x7ffef4de0168
READ of size 4 at 0x6040000000c0 thread T0
    #0 0xabd8c4 in ndlz8_decompress /src/c-blosc2/plugins/codecs/ndlz/ndlz8x8.c:457:3
    #1 0x5749c4 in blosc_d /src/c-blosc2/blosc/blosc2.c:1639:22
    #2 0x566527 in serial_blosc /src/c-blosc2/blosc/blosc2.c:1736:16
    #3 0x566527 in do_job /src/c-blosc2/blosc/blosc2.c:1901:15
    #4 0x56d64c in blosc_run_decompression_with_context /src/c-blosc2/blosc/blosc2.c:2541:13
    #5 0x56dd39 in blosc2_decompress /src/c-blosc2/blosc/blosc2.c:2609:12
    #6 0x55dcd6 in LLVMFuzzerTestOneInput /src/c-blosc2/tests/fuzz/fuzz_decompress_chunk.c:34:5
    #7 0x456c03 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x4424b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x447f65 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x470c62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7fcf355e00b2 in __libc_start_main
    #12 0x41f74d in _start

0x6040000000c0 is located 0 bytes to the right of 48-byte region [0x604000000090,0x6040000000c0)
allocated by thread T0 here:
    #0 0x524d6d in __interceptor_malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x4384f7 in operator new(unsigned long) cxa_noexception.cpp:0
    #2 0x4424b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #3 0x447f65 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #4 0x470c62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #5 0x7fcf355e00b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0xabd8c4)
Shadow bytes around the buggy address:
  0x0c087fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff8000: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
=>0x0c087fff8010: fa fa 00 00 00 00 00 00[fa]fa 00 00 00 00 00 00
  0x0c087fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==170707==ABORTING


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

==170707==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000000c0 at pc 0x000000abd8c5 bp 0x7ffef4de0170 sp 0x7ffef4de0168
READ of size 4 at 0x6040000000c0 thread T0
    #0 0xabd8c4  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0xabd8c4)
    #1 0x5749c4  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x5749c4)
    #2 0x566527  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x566527)
    #3 0x56d64c  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x56d64c)
    #4 0x56dd39  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x56dd39)
    #5 0x55dcd6  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x55dcd6)
    #6 0x456c03  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x456c03)
    #7 0x4424b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x4424b2)
    #8 0x447f65  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x447f65)
    #9 0x470c62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x470c62)
    #10 0x7fcf355e00b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #11 0x41f74d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x41f74d)

0x6040000000c0 is located 0 bytes to the right of 48-byte region [0x604000000090,0x6040000000c0)
allocated by thread T0 here:
    #0 0x524d6d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x524d6d)
    #1 0x4384f7  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x4384f7)
    #2 0x4424b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x4424b2)
    #3 0x447f65  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x447f65)
    #4 0x470c62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x470c62)
    #5 0x7fcf355e00b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (97 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer -rss_limit_mb=2560 -timeout=60
-runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/24a6684220b8301641f4ab3b1daca184f781b603b60a40d07c75fada3aff7d71
Time ran: 0.019989728927612305

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4097092354
INFO: Loaded 1 modules   (53183 inline 8-bit counters): 53183 [0xd10cc0, 0xd1dc7f),
INFO: Loaded 1 PC tables (53183 PCs): 53183 [0xbe67c0,0xcb63b0),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/24a6684220b8301641f4ab3b1daca184f781b603b60a40d07c75fada3aff7d71
=================================================================
==6738==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000000c0 at pc 0x000000abd8c5 bp 0x7ffd5a131830 sp 0x7ffd5a131828
READ of size 4 at 0x6040000000c0 thread T0
    #0 0xabd8c4 in ndlz8_decompress /src/c-blosc2/plugins/codecs/ndlz/ndlz8x8.c:457:3
    #1 0x5749c4 in blosc_d /src/c-blosc2/blosc/blosc2.c:1639:22
    #2 0x566527 in serial_blosc /src/c-blosc2/blosc/blosc2.c:1736:16
    #3 0x566527 in do_job /src/c-blosc2/blosc/blosc2.c:1901:15
    #4 0x56d64c in blosc_run_decompression_with_context /src/c-blosc2/blosc/blosc2.c:2541:13
    #5 0x56dd39 in blosc2_decompress /src/c-blosc2/blosc/blosc2.c:2609:12
    #6 0x55dcd6 in LLVMFuzzerTestOneInput /src/c-blosc2/tests/fuzz/fuzz_decompress_chunk.c:34:5
    #7 0x456c03 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #8 0x4424b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #9 0x447f65 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #10 0x470c62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #11 0x7f43bf7cf0b2 in __libc_start_main
    #12 0x41f74d in _start

0x6040000000c0 is located 0 bytes to the right of 48-byte region [0x604000000090,0x6040000000c0)
allocated by thread T0 here:
    #0 0x524d6d in __interceptor_malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x4384f7 in operator new(unsigned long) cxa_noexception.cpp:0
    #2 0x4424b2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #3 0x447f65 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #4 0x470c62 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #5 0x7f43bf7cf0b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0xabd8c4)
Shadow bytes around the buggy address:
  0x0c087fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff8000: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
=>0x0c087fff8010: fa fa 00 00 00 00 00 00[fa]fa 00 00 00 00 00 00
  0x0c087fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==6738==ABORTING


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

==6738==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000000c0 at pc 0x000000abd8c5 bp 0x7ffd5a131830 sp 0x7ffd5a131828
READ of size 4 at 0x6040000000c0 thread T0
    #0 0xabd8c4  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0xabd8c4)
    #1 0x5749c4  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x5749c4)
    #2 0x566527  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x566527)
    #3 0x56d64c  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x56d64c)
    #4 0x56dd39  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x56dd39)
    #5 0x55dcd6  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x55dcd6)
    #6 0x456c03  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x456c03)
    #7 0x4424b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x4424b2)
    #8 0x447f65  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x447f65)
    #9 0x470c62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x470c62)
    #10 0x7f43bf7cf0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #11 0x41f74d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x41f74d)

0x6040000000c0 is located 0 bytes to the right of 48-byte region [0x604000000090,0x6040000000c0)
allocated by thread T0 here:
    #0 0x524d6d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x524d6d)
    #1 0x4384f7  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x4384f7)
    #2 0x4424b2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x4424b2)
    #3 0x447f65  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x447f65)
    #4 0x470c62  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/c-blosc2_libfuzzer_asan/custom/c-blosc2/decompress_chunk_fuzzer+0x470c62)
    #5 0x7f43bf7cf0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

```
[2021-11-17 14:09:07 UTC] comput19-20211115-16:27: Fuzz task : Fuzzer libFuzzer_decompress_chunk_fuzzer generated testcase crashed in 412 seconds (r1).
[2021-11-17 14:10:45 UTC] comput19-20211115-16:27: Minimize task started.
[2021-11-17 14:35:31 UTC] comput19-20211115-16:27: Minimize task finished.
[2021-11-22 03:11:03 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:11:03 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.
```