Direct-leak · whine_malloc

Loaded 2 minutes ago

REDO TASK DELETE

OVERVIEW

Crash State:
```
whine_malloc
do_icmp_ping
address_allocate
```

Crash Type: Direct-leak
Created: Wed, Nov 17, 2021, 3:57 AM
Security: NO
Crash Address: ---
Sanitizer: address (ASAN)
Reliably Reproduces: YES
Issue: None
Platform: linux
Fuzzing Engine: libFuzzer
Fuzz Target: fuzz_dhcp
Job Type: dnsmasq_libfuzzer_asan
Project: test-project
Fixed: NO

Minimized Testcase: (2 KB) Unminimized Testcase: (3 KB) Re-upload Testcase: Build:

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

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (59 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp -rss_limit_mb=2560 -timeout=60 -runs=100 /clust
erfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/leak-57ab708ef478246a33d84d6dbb10d5e70acc8150
Time ran: 0.029302358627319336

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4183674705
INFO: Loaded 1 modules   (13271 inline 8-bit counters): 13271 [0x72da50, 0x730e27),
INFO: Loaded 1 PC tables (13271 PCs): 13271 [0x69a4f8,0x6ce268),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/leak-57ab708ef478246a33d84d6dbb10d5e70acc8150

=================================================================
==170201==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x525112 in __interceptor_calloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:138:3
    #1 0x62913e in whine_malloc /src/dnsmasq/src/util.c:331:15
    #2 0x577338 in do_icmp_ping /src/dnsmasq/src/dhcp.c:754:18
    #3 0x577be2 in address_allocate /src/dnsmasq/src/dhcp.c:841:16
    #4 0x60a723 in dhcp_reply /src/dnsmasq/src/rfc2131.c:626:11
    #5 0x57360b in dhcp_packet /src/dnsmasq/src/dhcp.c:354:21
    #6 0x5602ca in FuzzDhcp /src/fuzz_dhcp.c:41:3
    #7 0x56054e in LLVMFuzzerTestOneInput /src/fuzz_dhcp.c:78:3
    #8 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #9 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #10 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #11 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #12 0x7fc1861aa0b2 in __libc_start_main

================================================================================
The following leaks are not necessarily related to the first leak.


SUMMARY: AddressSanitizer: 32 byte(s) leaked in 1 allocation(s).

INFO: a leak has been found in the initial corpus.

INFO: to ignore leaks on libFuzzer side use -detect_leaks=0.


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

Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x525112  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x525112)
    #1 0x62913e  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x62913e)
```

```
    #2 0x577338  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x577338)
    #3 0x577be2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x577be2)
    #4 0x60a723  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x60a723)
    #5 0x57360b  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x57360b)
    #6 0x5602ca  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x5602ca)
    #7 0x56054e  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x56054e)
    #8 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x456e13)
    #9 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x4426c2)
    #10 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x448175)
    #11 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x470e72)
    #12 0x7fc1861aa0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (59 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+---------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp -rss_limit_mb=2560 -timeout=60 -runs=100 /clust
erfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/dd4f5e44f28b81656ff8d4ca6a6aea7ef478246a33d84d6dbb10d5e70acc8150
Time ran: 0.02337932586669922

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 3664690848
INFO: Loaded 1 modules   (13271 inline 8-bit counters): 13271 [0x72da50, 0x730e27),
INFO: Loaded 1 PC tables (13271 PCs): 13271 [0x69a4f8,0x6ce268),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/dd4f5e44f28b81656ff8d4ca6a6aea7ef478246a33d84d6dbb10d5e70acc8150

=================================================================
==197013==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x525112 in __interceptor_calloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:138:3
    #1 0x62913e in whine_malloc /src/dnsmasq/src/util.c:331:15
    #2 0x577338 in do_icmp_ping /src/dnsmasq/src/dhcp.c:754:18
    #3 0x577be2 in address_allocate /src/dnsmasq/src/dhcp.c:841:16
    #4 0x60a723 in dhcp_reply /src/dnsmasq/src/rfc2131.c:626:11
    #5 0x57360b in dhcp_packet /src/dnsmasq/src/dhcp.c:354:21
    #6 0x5602ca in FuzzDhcp /src/fuzz_dhcp.c:41:3
    #7 0x56054e in LLVMFuzzerTestOneInput /src/fuzz_dhcp.c:78:3
    #8 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #9 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #10 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #11 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #12 0x7f3d13dd00b2 in __libc_start_main

================================================================================
The following leaks are not necessarily related to the first leak.


SUMMARY: AddressSanitizer: 32 byte(s) leaked in 1 allocation(s).

INFO: a leak has been found in the initial corpus.

INFO: to ignore leaks on libFuzzer side use -detect_leaks=0.


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


Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x525112  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x525112)
    #1 0x62913e  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x62913e)
    #2 0x577338  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x577338)
    #3 0x577be2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x577be2)
    #4 0x60a723  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x60a723)
    #5 0x57360b  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x57360b)
    #6 0x5602ca  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x5602ca)
    #7 0x56054e  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x56054e)
    #8 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x456e13)
    #9 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x4426c2)
    #10 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x448175)
    #11 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_dhcp+0x470e72)
    #12 0x7f3d13dd00b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-16 19:57:14 UTC] comput17-20211115-16:27: Fuzz task : Fuzzer libFuzzer_fuzz_dhcp generated testcase crashed in 25 seconds (r1).
[2021-11-16 20:08:31 UTC] comput14-20211115-16:27: Minimize task started.
[2021-11-16 20:34:34 UTC] comput14-20211115-16:27: Minimize task finished.
[2021-11-22 03:10:59 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:59 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.