Heap-buffer-overflow WRITE 1 · extract_name

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State: `extract_name`
`hash_questions`
`fuzz_util.c`

Crash Type:	Heap-buffer-overflow WRITE 1	Created:	Mon, Nov 15, 2021, 7:47 PM	Security:	**YES (High)**
Crash Address:	0x607000000dfc	Sanitizer:	address (ASAN)	Reliably Reproduces:	YES
Issue:	None	Platform:	linux		
Fuzzing Engine:	libFuzzer	Fuzz Target:	fuzz_util	Job Type:	dnsmasq_libfuzzer_asan
Project:	test-project				
Fixed:	NO				

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

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

CRASH STACKTRACE

--- LAST TESTED STACKTRACE (94 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-57f64693e62aae311506a66f7e4962d7f47347aa
Time ran: 0.02053356170654297

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4166245790
INFO: Loaded 1 modules   (13282 inline 8-bit counters): 13282 [0x72da50, 0x730e32),
INFO: Loaded 1 PC tables (13282 PCs): 13282 [0x69a558,0x6ce378),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-57f64693e62aae311506a66f7e4962d7f47347aa
=================================================================
==168312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000dfc at pc 0x0000005d7ece bp 0x7ffe59662f20 sp 0x7ffe59662f18
WRITE of size 1 at 0x607000000dfc thread T0
    #0 0x5d7ecd in extract_name /src/dnsmasq/src/rfc1035.c:106:11
    #1 0x584d7e in hash_questions /src/dnsmasq/src/hash-questions.c:111:12
    #2 0x560739 in LLVMFuzzerTestOneInput /src/fuzz_util.c:53:9
    #3 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #4 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #5 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #6 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #7 0x7fe2756bc0b2 in __libc_start_main
    #8 0x41f95d in _start

0x607000000dfc is located 0 bytes to the right of 76-byte region [0x607000000db0,0x607000000dfc)
allocated by thread T0 here:
    #0 0x524f7d in malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x5604b8 in get_null_terminated /src/fuzz_header.h:47:17
    #2 0x5604b8 in gb_get_null_terminated /src/fuzz_header.h:74:16
    #3 0x5604b8 in LLVMFuzzerTestOneInput /src/fuzz_util.c:22:16
    #4 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #5 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #6 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #7 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #8 0x7fe2756bc0b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x5d7ecd)
Shadow bytes around the buggy address:
  0x0c0e7fff8160: fa fa 00 00 00 00 00 00 00 00 04 fa fa fa fa
  0x0c0e7fff8170: 00 00 00 00 00 00 00 00 00 04 fa fa fa fa 00 00
  0x0c0e7fff8180: 00 00 00 00 00 00 00 04 fa fa fa fa 00 00 00 00
  0x0c0e7fff8190: 00 00 00 00 00 04 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff81a0: 00 00 00 04 fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c0e7fff81b0: 00 04 fa fa fa fa 00 00 00 00 00 00 00 00[04]
  0x0c0e7fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8200: 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
==168312==ABORTING


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

==168312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000dfc at pc 0x0000005d7ece bp 0x7ffe59662f20 sp 0x7ffe59662f18
WRITE of size 1 at 0x607000000dfc thread T0
    #0 0x5d7ecd  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x5d7ecd)
    #1 0x584d7e  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x584d7e)
    #2 0x560739  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x560739)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x470e72)
    #7 0x7fe2756bc0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x41f95d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x41f95d)

0x607000000dfc is located 0 bytes to the right of 76-byte region [0x607000000db0,0x607000000dfc)
allocated by thread T0 here:
    #0 0x524f7d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x524f7d)
    #1 0x5604b8  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x5604b8)
    #2 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x456e13)
    #3 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x4426c2)
    #4 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x448175)
    #5 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x470e72)
    #6 0x7fe2756bc0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (94 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/2e429b36e04863147fddbca4acaa1f5be62aae311506a66f7e4962d7f47347aa
Time ran: 0.017244338989257812

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 3244685888
INFO: Loaded 1 modules   (13282 inline 8-bit counters): 13282 [0x72da50, 0x730e32),
INFO: Loaded 1 PC tables (13282 PCs): 13282 [0x69a558,0x6ce378),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/2e429b36e04863147fddbca4acaa1f5be62aae311506a66f7e4962d7f47347aa
=================================================================
==184328==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000dfc at pc 0x0000005d7ece bp 0x7ffdbefe0e00 sp 0x7ffdbefe0df8
WRITE of size 1 at 0x607000000dfc thread T0
    #0 0x5d7ecd in extract_name /src/dnsmasq/src/rfc1035.c:106:11
    #1 0x584d7e in hash_questions /src/dnsmasq/src/hash-questions.c:111:12
    #2 0x560739 in LLVMFuzzerTestOneInput /src/fuzz_util.c:53:9
    #3 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #4 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #5 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #6 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #7 0x7f1d62eeb0b2 in __libc_start_main
    #8 0x41f95d in _start

```

```
0x607000000dfc is located 0 bytes to the right of 76-byte region [0x607000000db0,0x607000000dfc)
allocated by thread T0 here:
    #0 0x524f7d in malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x5604b8 in get_null_terminated /src/fuzz_header.h:47:17
    #2 0x5604b8 in gb_get_null_terminated /src/fuzz_header.h:74:16
    #3 0x5604b8 in LLVMFuzzerTestOneInput /src/fuzz_util.c:22:16
    #4 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #5 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #6 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #7 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #8 0x7f1d62eeb0b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x5d7ecd)
Shadow bytes around the buggy address:
  0x0c0e7fff8160: fa fa 00 00 00 00 00 00 00 00 00 04 fa fa fa fa
  0x0c0e7fff8170: 00 00 00 00 00 00 00 00 00 04 fa fa fa fa 00 00
  0x0c0e7fff8180: 00 00 00 00 00 00 00 04 fa fa fa fa 00 00 00 00
  0x0c0e7fff8190: 00 00 00 00 00 04 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff81a0: 00 00 00 04 fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c0e7fff81b0: 00 04 fa fa fa fa 00 00 00 00 00 00 00 00[04]
  0x0c0e7fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8200: 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
==184328==ABORTING


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

==184328==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000dfc at pc 0x0000005d7ece bp 0x7ffdbefe0e00 sp 0x7ffdbefe0df8
WRITE of size 1 at 0x607000000dfc thread T0
    #0 0x5d7ecd  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x5d7ecd)
    #1 0x584d7e  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x584d7e)
    #2 0x560739  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x560739)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x470e72)
    #7 0x7f1d62eeb0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x41f95d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x41f95d)

0x607000000dfc is located 0 bytes to the right of 76-byte region [0x607000000db0,0x607000000dfc)
allocated by thread T0 here:
    #0 0x524f7d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x524f7d)
    #1 0x5604b8  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x5604b8)
    #2 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x456e13)
    #3 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x4426c2)
    #4 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x448175)
    #5 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_util+0x470e72)
    #6 0x7f1d62eeb0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

```
[2021-11-15 11:47:10 UTC] comput4-20211115-16:27: Fuzz task : Fuzzer libFuzzer_fuzz_util generated testcase crashed in 5 seconds (r1).
[2021-11-15 11:48:48 UTC] comput3-20211115-16:27: Minimize task started.
[2021-11-15 12:14:49 UTC] comput3-20211115-16:27: Minimize task finished.
[2021-11-22 03:10:41 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:42 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.
```