Heap-buffer-overflow WRITE 1 · check_bad_address

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State: check_bad_address
check_for_bogus_wildcard
FuzzCheckForBogusWildcard

Crash Type: Heap-buffer-overflow WRITE 1

Created: Mon, Nov 15, 2021, 4:29 PM

Security: **YES (High)**

Crash Address: 0x607000000d8c

Sanitizer: address (ASAN)

Reliably Reproduces: YES

Issue: None

Platform: linux

Fuzzing Engine: libFuzzer

Fuzz Target: fuzz_rfc1035

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 (99 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035 -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-9a5aad5af4ead3165becefc79f0958ad4b70eebd
Time ran: 0.02106952667236328

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4165268010
INFO: Loaded 1 modules   (13334 inline 8-bit counters): 13334 [0x72fa50, 0x732e66),
INFO: Loaded 1 PC tables (13334 PCs): 13334 [0x69b578,0x6cf6d8),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-9a5aad5af4ead3165becefc79f0958ad4b70eebd
=================================================================
==168186==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000d8c at pc 0x0000005f3697 bp 0x7ffedf3afcd0 sp 0x7ffedf3afcc8
WRITE of size 1 at 0x607000000d8c thread T0
    #0 0x5f3696 in extract_name /src/dnsmasq/src/rfc1035.c:106:11
    #1 0x5f3696 in check_bad_address /src/dnsmasq/src/rfc1035.c:1151:20
    #2 0x5f2330 in check_for_bogus_wildcard /src/dnsmasq/src/rfc1035.c:1209:7
    #3 0x561341 in FuzzCheckForBogusWildcard /src/fuzz_rfc1035.c:204:5
    #4 0x5619b8 in LLVMFuzzerTestOneInput /src/fuzz_rfc1035.c:258:7
    #5 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #6 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #7 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #8 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #9 0x7f5bd1a760b2 in __libc_start_main
    #10 0x41f95d in _start

0x607000000d8c is located 0 bytes to the right of 76-byte region [0x607000000d40,0x607000000d8c)
allocated by thread T0 here:
    #0 0x524f7d in malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x56120a in get_null_terminated /src/fuzz_header.h:47:17
    #2 0x56120a in gb_get_null_terminated /src/fuzz_header.h:74:16
    #3 0x56120a in FuzzCheckForBogusWildcard /src/fuzz_rfc1035.c:190:17
    #4 0x5619b8 in LLVMFuzzerTestOneInput /src/fuzz_rfc1035.c:258:7
    #5 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #6 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #7 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #8 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #9 0x7f5bd1a760b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5f3696)
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 fa fa fa fa fa fa fa fa fa fa
```

```
  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
==168186==ABORTING


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

==168186==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000d8c at pc 0x0000005f3697 bp 0x7ffedf3afcd0 sp 0x7ffedf3afcc8
WRITE of size 1 at 0x607000000d8c thread T0
    #0 0x5f3696  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5f3696)
    #1 0x5f2330  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5f2330)
    #2 0x561341  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x561341)
    #3 0x5619b8  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5619b8)
    #4 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x456e13)
    #5 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x4426c2)
    #6 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x448175)
    #7 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x470e72)
    #8 0x7f5bd1a760b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #9 0x41f95d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x41f95d)

0x607000000d8c is located 0 bytes to the right of 76-byte region [0x607000000d40,0x607000000d8c)
allocated by thread T0 here:
    #0 0x524f7d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x524f7d)
    #1 0x56120a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x56120a)
    #2 0x5619b8  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5619b8)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x470e72)
    #7 0x7f5bd1a760b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

--- ORIGINAL STACKTRACE ON **REVISION 1** (99 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035 -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/9284bd6b3e1c4b888acb7429cca0cfa7f4ead3165becefc79f0958ad4b70eebd
Time ran: 0.01670050621032715

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4286110883
INFO: Loaded 1 modules   (13334 inline 8-bit counters): 13334 [0x72fa50, 0x732e66),
INFO: Loaded 1 PC tables (13334 PCs): 13334 [0x69b578,0x6cf6d8),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/9284bd6b3e1c4b888acb7429cca0cfa7f4ead3165becefc79f0958ad4b70eebd
=================================================================
==2152==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000d8c at pc 0x0000005f3697 bp 0x7ffdf0b55570 sp 0x7ffdf0b55568
WRITE of size 1 at 0x607000000d8c thread T0
    #0 0x5f3696 in extract_name /src/dnsmasq/src/rfc1035.c:106:11
    #1 0x5f3696 in check_bad_address /src/dnsmasq/src/rfc1035.c:1151:20
    #2 0x5f2330 in check_for_bogus_wildcard /src/dnsmasq/src/rfc1035.c:1209:7
    #3 0x561341 in FuzzCheckForBogusWildcard /src/fuzz_rfc1035.c:204:5
    #4 0x5619b8 in LLVMFuzzerTestOneInput /src/fuzz_rfc1035.c:258:7
    #5 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #6 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #7 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #8 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #9 0x7f4db9d210b2 in __libc_start_main
    #10 0x41f95d in _start

0x607000000d8c is located 0 bytes to the right of 76-byte region [0x607000000d40,0x607000000d8c)
allocated by thread T0 here:
    #0 0x524f7d in malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x56120a in get_null_terminated /src/fuzz_header.h:47:17
    #2 0x56120a in gb_get_null_terminated /src/fuzz_header.h:74:16
    #3 0x56120a in FuzzCheckForBogusWildcard /src/fuzz_rfc1035.c:190:17
    #4 0x5619b8 in LLVMFuzzerTestOneInput /src/fuzz_rfc1035.c:258:7
    #5 0x456e13 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) cxa_noexception.cpp:0
    #6 0x4426c2 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #7 0x448175 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) cxa_noexception.cpp:0
    #8 0x470e72 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #9 0x7f4db9d210b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5f3696)
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 fa fa fa fa fa fa fa fa fa fa
  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
==2152==ABORTING


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

==2152==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000d8c at pc 0x0000005f3697 bp 0x7ffdf0b55570 sp 0x7ffdf0b55568
WRITE of size 1 at 0x607000000d8c thread T0
    #0 0x5f3696  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5f3696)
    #1 0x5f2330  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5f2330)
    #2 0x561341  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x561341)
    #3 0x5619b8  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5619b8)
    #4 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x456e13)
    #5 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x4426c2)
    #6 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x448175)
    #7 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x470e72)
    #8 0x7f4db9d210b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #9 0x41f95d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x41f95d)

0x607000000d8c is located 0 bytes to the right of 76-byte region [0x607000000d40,0x607000000d8c)
allocated by thread T0 here:
    #0 0x524f7d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x524f7d)
    #1 0x56120a  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x56120a)
    #2 0x5619b8  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x5619b8)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_rfc1035+0x470e72)
    #7 0x7f4db9d210b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

```
[2021-11-15 08:29:11 UTC] comput6-20211115-16:27: Fuzz task : Fuzzer libFuzzer_fuzz_rfc1035 generated testcase crashed in 14 seconds (r1).
[2021-11-15 08:31:25 UTC] comput13-20211115-16:27: Minimize task started.
[2021-11-15 08:57:26 UTC] comput13-20211115-16:27: Minimize task finished.
[2021-11-22 03:10:40 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:10:41 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.
```