Heap-buffer-overflow WRITE 1 · extract_name

Loaded just now

REDO TASK DELETE

OVERVIEW

Crash State: extract_name
answer_auth
fuzz_auth.c

Crash Type: Heap-buffer-overflow WRITE 1

Created: Wed, Nov 17, 2021, 11:34 AM

Security: **YES (High)**

Crash Address: 0x60700000006c

Sanitizer: address (ASAN)

Reliably Reproduces: YES

Issue: None

Platform: linux

Fuzzing Engine: libFuzzer

Fuzz Target: fuzz_auth

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 (97 LINES) ---

```
[Environment] ASAN_OPTIONS=exitcode=77
+----------------------------------------Release Build Stacktrace----------------------------------------+
Command: /clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-8cd400eb65f39afaf1c8cd34516a4a320b3269d2
Time ran: 0.021148681640625

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 4185569125
INFO: Loaded 1 modules   (13282 inline 8-bit counters): 13282 [0x72da50, 0x730e32),
INFO: Loaded 1 PC tables (13282 PCs): 13282 [0x69a578,0x6ce398),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/crash-8cd400eb65f39afaf1c8cd34516a4a320b3269d2
=================================================================
==170455==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000006c at pc 0x0000005f490e bp 0x7ffdf1189aa0 sp 0x7ffdf1189a98
WRITE of size 1 at 0x60700000006c thread T0
    #0 0x5f490d in extract_name /src/dnsmasq/src/rfc1035.c:106:11
    #1 0x561121 in answer_auth /src/dnsmasq/src/auth.c:140:12
    #2 0x5608ad in FuzzAuth /src/fuzz_auth.c:35:3
    #3 0x5608ad in LLVMFuzzerTestOneInput /src/fuzz_auth.c:62:3
    #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 0x7f8223f9b0b2 in __libc_start_main
    #9 0x41f95d in _start

0x60700000006c is located 0 bytes to the right of 76-byte region [0x607000000020,0x60700000006c)
allocated by thread T0 here:
    #0 0x524f7d in malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x55ca30 in get_null_terminated /src/fuzz_header.h:47:17
    #2 0x55ca30 in gb_get_null_terminated /src/fuzz_header.h:74:16
    #3 0x55ca30 in init_daemon /src/fuzz_header.h:238:27
    #4 0x5606bb in LLVMFuzzerTestOneInput /src/fuzz_auth.c:56:14
    #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 0x7f8223f9b0b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5f490d)
Shadow bytes around the buggy address:
  0x0c0e7fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00[04]fa fa
  0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 04 fa fa fa fa
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 04 fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 04 fa fa fa fa 00 00 00 00
  0x0c0e7fff8040: 00 00 00 00 00 04 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff8050: 00 00 00 04 fa fa fa fa 00 00 00 00 00 00 00 00
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
==170455==ABORTING


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

==170455==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000006c at pc 0x0000005f490e bp 0x7ffdf1189aa0 sp 0x7ffdf1189a98
WRITE of size 1 at 0x60700000006c thread T0
    #0 0x5f490d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5f490d)
    #1 0x561121  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x561121)
    #2 0x5608ad  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5608ad)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x470e72)
    #7 0x7f8223f9b0b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x41f95d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x41f95d)

0x60700000006c is located 0 bytes to the right of 76-byte region [0x607000000020,0x60700000006c)
allocated by thread T0 here:
    #0 0x524f7d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x524f7d)
    #1 0x55ca30  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x55ca30)
    #2 0x5606bb  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5606bb)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x470e72)
    #7 0x7f8223f9b0b2  (/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/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth -rss_limit_mb=2560 -timeout=60 -runs=100 /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/0d88949dcbfdb54c86189768470a7f4165f39afaf1c8cd34516a4a320b3269d2
Time ran: 0.018287181854248047

INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 976252991
INFO: Loaded 1 modules   (13282 inline 8-bit counters): 13282 [0x72da50, 0x730e32),
INFO: Loaded 1 PC tables (13282 PCs): 13282 [0x69a578,0x6ce398),
/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth: Running 1 inputs 100 time(s) each.
Running: /clusterfuzz/run_bot/clusterfuzz/bot/inputs/fuzzer-testcases/0d88949dcbfdb54c86189768470a7f4165f39afaf1c8cd34516a4a320b3269d2
=================================================================
==86066==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000006c at pc 0x0000005f490e bp 0x7ffc92041760 sp 0x7ffc92041758
WRITE of size 1 at 0x60700000006c thread T0
    #0 0x5f490d in extract_name /src/dnsmasq/src/rfc1035.c:106:11
    #1 0x561121 in answer_auth /src/dnsmasq/src/auth.c:140:12
    #2 0x5608ad in FuzzAuth /src/fuzz_auth.c:35:3
    #3 0x5608ad in LLVMFuzzerTestOneInput /src/fuzz_auth.c:62:3
    #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 0x7f6e45b960b2 in __libc_start_main
    #9 0x41f95d in _start

0x60700000006c is located 0 bytes to the right of 76-byte region [0x607000000020,0x60700000006c)
allocated by thread T0 here:
    #0 0x524f7d in malloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:129:3
    #1 0x55ca30 in get_null_terminated /src/fuzz_header.h:47:17
    #2 0x55ca30 in gb_get_null_terminated /src/fuzz_header.h:74:16
    #3 0x55ca30 in init_daemon /src/fuzz_header.h:238:27
    #4 0x5606bb in LLVMFuzzerTestOneInput /src/fuzz_auth.c:56:14
    #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 0x7f6e45b960b2 in __libc_start_main

SUMMARY: AddressSanitizer: heap-buffer-overflow (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5f490d)
Shadow bytes around the buggy address:
  0x0c0e7fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00[04]fa fa
  0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 04 fa fa fa fa
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 04 fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 04 fa fa fa fa 00 00 00 00
  0x0c0e7fff8040: 00 00 00 00 00 04 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff8050: 00 00 00 04 fa fa fa fa 00 00 00 00 00 00 00 00
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
==86066==ABORTING


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

==86066==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000006c at pc 0x0000005f490e bp 0x7ffc92041760 sp 0x7ffc92041758
WRITE of size 1 at 0x60700000006c thread T0
    #0 0x5f490d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5f490d)
    #1 0x561121  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x561121)
    #2 0x5608ad  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5608ad)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x470e72)
    #7 0x7f6e45b960b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x41f95d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x41f95d)

0x60700000006c is located 0 bytes to the right of 76-byte region [0x607000000020,0x60700000006c)
allocated by thread T0 here:
    #0 0x524f7d  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x524f7d)
    #1 0x55ca30  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x55ca30)
    #2 0x5606bb  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x5606bb)
    #3 0x456e13  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x456e13)
    #4 0x4426c2  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x4426c2)
    #5 0x448175  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x448175)
    #6 0x470e72  (/clusterfuzz/run_bot/clusterfuzz/bot/builds/dnsmasq_libfuzzer_asan/custom/dnsmasq/fuzz_auth+0x470e72)
    #7 0x7f6e45b960b2  (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
```

TESTCASE ANALYSIS ON OTHER JOBS

No reproducible variants found.

METADATA

[2021-11-17 03:34:53 UTC] comput8-20211115-16:27: Fuzz task : Fuzzer libFuzzer_fuzz_auth generated testcase crashed in 3 seconds (r1).
[2021-11-17 03:44:48 UTC] comput19-20211115-16:27: Minimize task started.
[2021-11-17 04:10:50 UTC] comput19-20211115-16:27: Minimize task finished.
[2021-11-22 03:11:01 UTC] comput4-20211115-16:27: Progression task started.
[2021-11-22 03:11:01 UTC] comput4-20211115-16:27: Progression task finished: still crashes on latest custom build.