AddressSanitizer: heap-use-after-free in error() modules/preprocs/nasm/nasm-pp.c:4830 #162

⊙ Open **Clingto** opened this issue on May 19, 2021 · 0 comments

Clingto commented on May 19, 2021

System info:
Ubuntu 16.04.6 LTS, X64, gcc 5.4.0, yasm (latest master `009450c`)
Compile Command:

```
$ ./autogen.sh
make distclean

CC=gcc CXX=g++ CFLAGS="-fsanitize=address -fno-omit-frame-pointer -g" CXXFLAGS="-fsanitize=address -fno-omit-frame-pointer -g" ./configure --prefix=$PWD/build --disable-shared
make -j
make install
```

Run Command:

```
$ yasm  $POC
```

POC file:
https://github.com/Clingto/POC/blob/master/MSA/yasm/yasm-4826-error-UAF

ASAN info:

```
yasm: file name already has no extension: output will be in `yasm.out'
=================================================================
==17967==ERROR: AddressSanitizer: heap-use-after-free on address 0x60e00000cd08 at pc 0x7f820a4aa94b bp 0x7ffd4c279450 sp 0x7ffd4c279440
READ of size 8 at 0x60e00000cd08 thread T0
    #0 0x7f820a4aa94a in error  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:4830
    #1 0x7f820a4aceaf in tokenise  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:1352
    #2 0x7f820a4c0300 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5037
    #3 0x7f820a4a9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #4 0x7f820a49b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #5 0x7f820a48f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #6 0x7f820a48f36b in nasm_parser_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
    #7 0x402c84 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
    #8 0x402c84 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #9 0x7f820d6ae82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #10 0x403ee8 in _start ( test/yasm-uaf/bin_asan/bin/yasm+0x403ee8)

0x60e00000cd08 is located 8 bytes inside of 160-byte region [0x60e00000cd00,0x60e00000cda0)
freed by thread T0 here:
    #0 0x7f820df682ca in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x982ca)
    #1 0x7f820a4bfd48 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5009
    #2 0x7f820a4a9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #3 0x7f820a49b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #4 0x7f820a48f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #5 0x7f820a48f36b in nasm_parser_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
    #6 0x402c84 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
    #7 0x402c84 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #8 0x7f820d6ae82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

previously allocated by thread T0 here:
    #0 0x7f820df68602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x7f820dcb9769 in def_xmalloc  test/yasm-uaf/SRC_asan/libyasm/xmalloc.c:69
    #2 0x7f820a4b500b in do_directive  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:3211
    #3 0x7f820a4c0333 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5083
    #4 0x7f820a4a9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #5 0x7f820a49b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #6 0x7f820a48f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #7 0x7f820a48f36b in nasm_parser_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:83
    #8 0x402c84 in do_assemble  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:521
    #9 0x402c84 in main  test/yasm-uaf/SRC_asan/frontends/yasm/yasm.c:753
    #10 0x7f820d6ae82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: heap-use-after-free  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:4830 error
Shadow bytes around the buggy address:
  0x0c1c7fff9950: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff9960: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff9970: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff9980: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1c7fff9990: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
=>0x0c1c7fff99a0: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1c7fff99b0: fd fd fd fd fa fa fa fa fa fa fa fa 00 00 00 00
  0x0c1c7fff99c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff99d0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c1c7fff99e0: 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c1c7fff99f0: fa fa fa fa 00 00 00 00 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==17967==ABORTING
```

👎 1

natalie13m mentioned this issue on Nov 1, 2021

Stack overflow in parse_expr6(5,4,3,2,1) modules/parsers/nasm/nasm-parse.c #152

⊙ Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant