New issue

Jump to bottom

A NULL pointer dereference in the function expand_mmac_params() modules/preprocs/nasm/nasm-pp.c:3861 #171

Open **Clingto** opened this issue on May 19, 2021 · 1 comment

Clingto commented on May 19, 2021

System info:
Ubuntu 16.04.6 LTS, X64, gcc 5.4.0, yasm (latest master `009450c`)
I think it is probably a similar issue as #151
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-3857-expand_mmac_params-null-pointer-deref

ASAN info:

```
yasm: file name already has no extension: output will be in `yasm.out'
ASAN:SIGSEGV
=================================================================
==15506==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000001 (pc 0x7fc6c3caf512 bp 0x7ffceebde200 sp 0x7ffceebde060 T0)
    #0 0x7fc6c3caf511 in expand_mmac_params  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:3861
    #1 0x7fc6c3cc08e8 in pp_getline  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:5078
    #2 0x7fc6c3ca9d46 in nasm_preproc_get_line  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-preproc.c:198
    #3 0x7fc6c3c9b2ac in nasm_parser_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parse.c:218
    #4 0x7fc6c3c8f36b in nasm_do_parse  test/yasm-uaf/SRC_asan/modules/parsers/nasm/nasm-parser.c:66
    #5 0x7fc6c3c8f36b 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 0x7fc6c6db382f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #9 0x403ee8 in _start ( test/yasm-uaf/bin_asan/bin/yasm+0x403ee8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV  test/yasm-uaf/SRC_asan/modules/preprocs/nasm/nasm-pp.c:3861 expand_mmac_params
==15506==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

ArchanaYocto commented on Oct 20

I attempted to reproduce the issue using host : ubuntu 22.04 which has gcc-11.2.0 but i don't see the same error.

I am using : `101bca9` (HEAD -> master, origin/master, origin/HEAD) Add vcpkg installation instructions (#200)

I see:

yasm-3857-expand_mmac_params-null-pointer-deref:1540: error: label or instruction expected at start of line
yasm-3857-expand_mmac_params-null-pointer-deref:1540: warning: ignoring unrecognized character `<' `yasm-3857-expand_mmac_params-null-pointer-deref:1540: warning: ignoring unrecognized character `>'`

```
=================================================================
==2306410==ERROR: LeakSanitizer: detected memory leaks
```

Direct leak of 4100 byte(s) in 4 object(s) allocated from:
#0 0x560053dd0207 in malloc (/buildarea/eng3/yasm/yasm/build/bin/yasm+0x13b207)
#1 0x560053e52d14 in def_xmalloc libyasm/xmalloc.c:69
#2 0x560053e2fd18 in yasm_error_set_va libyasm/errwarn.c:277
#3 0x560053e2fe7e in yasm_error_set libyasm/errwarn.c:289
#4 0x560053e80465 in expect_ modules/parsers/nasm/nasm-parse.c:208
#5 0x560053e84508 in parse_instr modules/parsers/nasm/nasm-parse.c:769
#6 0x560053e82f8c in parse_exp modules/parsers/nasm/nasm-parse.c:567
#7 0x560053e80e54 in parse_line modules/parsers/nasm/nasm-parse.c:290
#8 0x560053e80729 in nasm_parser_parse modules/parsers/nasm/nasm-parse.c:232
#9 0x560053e7f7a0 in nasm_do_parse modules/parsers/nasm/nasm-parser.c:66
#10 0x560053e7f93d in nasm_parser_do_parse modules/parsers/nasm/nasm-parser.c:83
#11 0x560053e176bc in do_assemble frontends/yasm/yasm.c:522
#12 0x560053e184e4 in main frontends/yasm/yasm.c:754
#13 0x7f7bfca7dd8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58

Direct leak of 4100 byte(s) in 4 object(s) allocated from:
#0 0x560053dd0207 in malloc (/buildarea/eng3/yasm/yasm/build/bin/yasm+0x13b207)
#1 0x560053e52d14 in def_xmalloc libyasm/xmalloc.c:69
#2 0x560053e2fd18 in yasm_error_set_va libyasm/errwarn.c:277
#3 0x560053e2fe7e in yasm_error_set libyasm/errwarn.c:289
#4 0x560053e80465 in expect_ modules/parsers/nasm/nasm-parse.c:208
#5 0x560053e84508 in parse_instr modules/parsers/nasm/nasm-parse.c:769
#6 0x560053e82f8c in parse_exp modules/parsers/nasm/nasm-parse.c:567
#7 0x560053e825bc in parse_line modules/parsers/nasm/nasm-parse.c:455
#8 0x560053e80729 in nasm_parser_parse modules/parsers/nasm/nasm-parse.c:232
#9 0x560053e7f7a0 in nasm_do_parse modules/parsers/nasm/nasm-parser.c:66
#10 0x560053e7f93d in nasm_parser_do_parse modules/parsers/nasm/nasm-parser.c:83
#11 0x560053e176bc in do_assemble frontends/yasm/yasm.c:522
#12 0x560053e184e4 in main frontends/yasm/yasm.c:754
#13 0x7f7bfca7dd8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58

SUMMARY: AddressSanitizer: 8200 byte(s) leaked in 8 allocation(s).

This is not same error as reported in this bug

I am able to spend some time to resolve some Yasm CVEs but I would need some guidance .
I have worked on C code for four years and have used Valgrind, but never used Address Sanitzer
Also I have more experienced developers to consult on this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants