Bug 3392708 - SEGV in tok_text asm/preproc.c:322

Status: CLOSED FIXED
Alias: None
Product: NASM
Component: Assembler (show other bugs)
Version: 2.15.xx
Hardware: All All
Importance: High critical
Assignee: nobody
URL:
Depends on:
Blocks:

Reported: 2020-07-28 04:05 PDT by Suhwan
Modified: 2020-07-30 15:58 PDT (History)
CC List: 5 users (show)
Obtained from: Build from source archive using configure

Attachments

poc (360 bytes, application/octet-stream) 2020-07-28 04:05 PDT, Suhwan	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

Suhwan 2020-07-28 04:05:42 PDT — Description

```
Created attachment 411797 [details]
poc

Hi,
I found a SEGV in tok_text asm/preproc.c:322
It is triggered in nasm version 2.15rc10.

Please run following command
`nasm -f win64 -o tmp.o $PoC`


==32505==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000c (pc
0x55f65853fe00 bp 0x7feb4656d600 sp 0x7ffed04f1fe0 T0)
==32505==The signal is caused by a READ memory access.
==32505==Hint: address points to the zero page.
    #0 0x55f65853fdff in tok_text asm/preproc.c:322
    #1 0x55f65853fdff in do_directive asm/preproc.c:3552
    #2 0x55f65855f738 in pp_tokline asm/preproc.c:6716
    #3 0x55f65855f738 in pp_getline asm/preproc.c:6779
    #4 0x55f6583d1dfa in assemble_file asm/nasm.c:1705
    #5 0x55f6583c7056 in main asm/nasm.c:712
    #6 0x7feb450f7b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #7 0x55f6583ca129 in _start
(/mnt/hda2/suhwan/add_project/final/FINAL_TEST_ZONE/program/nasm-
2.15rc10/install_dir/bin/nasm+0x124129)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV asm/preproc.c:322 in tok_text
==32505==ABORTING
```

Suhwan 2020-07-28 23:14:42 PDT — Comment 1

```
Still reproduced in NASM version 2.16rc0.
This is found by Agency for Defense Development (ADD) in South Korea.
```

H. Peter Anvin 2020-07-29 00:28:28 PDT — Comment 2

```
2.16rc0 is not an actual version, it is the tag for the future 2.16 development
branch, which is not up to date as focus is currently on the nasm-2.15.xx
maintenance branch.

The best would be if you can give the git ID for what you test, otherwise the daily
snapshot number.
```

Suhwan 2020-07-29 00:46:17 PDT — Comment 3

```
NASM version 2.15.04rc1 compiled on Jul 29 2020


==26762==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000c (pc
0x564f19a4e52c bp 0x7ff982d25640 sp 0x7ffd85154120 T0)
==26762==The signal is caused by a READ memory access.
==26762==Hint: address points to the zero page.
    #0 0x564f19a4e52b in tok_text asm/preproc.c:334
    #1 0x564f19a4e52b in do_directive asm/preproc.c:3671
    #2 0x564f19a6c19c in pp_tokline asm/preproc.c:6851
    #3 0x564f19a6c19c in pp_getline asm/preproc.c:6914
    #4 0x564f198e038b in assemble_file asm/nasm.c:1718
    #5 0x564f198d7171 in main asm/nasm.c:714
    #6 0x7ff9818afb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #7 0x564f198da289 in _start
(/mnt/hda2/suhwan/add_project/final/FINAL_TEST_ZONE/program/nasm-
2.15.04rc1/install_dir/bin/nasm+0x12a289)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV asm/preproc.c:334 in tok_text
==26762==ABORTING

Sorry for bothering you.
```

H. Peter Anvin 2020-07-30 15:58:58 PDT — Comment 4

```
Fixed in checkin 6299a3114ce0f3acd55d07de201a8ca2f0a83059
```