# Bug 3392712 - double-free in pp_tokline asm/preproc.c:6750

**Status:** CLOSED FIXED
**Alias:** None
**Product:** NASM
**Component:** Assembler (show other bugs)
**Version:** 2.15.xx
**Hardware:** All All
**Importance:** Medium normal
**Assignee:** nobody
**URL:**
**Duplicates (2):** ~~3392670~~ ~~3392671~~ (view as bug list)
**Depends on:**
**Blocks:**

**Reported:** 2020-08-03 22:11 PDT by Suhwan
**Modified:** 2020-08-18 06:45 PDT (History)
**CC List:** 5 users (show)

**Obtained from:** Build from source archive using configure

| Attachments | |
|---|---|
| **poc** (1.00 KB, text/x-matlab)<br>2020-08-03 22:11 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 2020-08-03 22:11:08 PDT Description

Created attachment 411800 [details]
poc

Hi, we found a double-free in pp_tokline asm/preproc.c:6750
version : nasm-2.15.04rc3

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

```
==32583==ERROR: AddressSanitizer: attempting double-free on 0x60c0001d7700 in
thread T0:
    #0 0x7fb5dfbf97a8 in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xde7a8)
    #1 0x556ecf725656 in nasm_free nasmlib/alloc.c:108
    #2 0x556ecf769767 in pp_tokline asm/preproc.c:6750
    #3 0x556ecf76a802 in pp_getline asm/preproc.c:6922
    #4 0x556ecf7231dc in assemble_file asm/nasm.c:1718
    #5 0x556ecf71e567 in main asm/nasm.c:714
    #6 0x7fb5df74bb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #7 0x556ecf71b809 in _start
(/mnt/hda2/suhwan/add_project/final/FINAL_TEST_ZONE/program/nasm-
2.15.04rc3/install_dir/bin/nasm+0x111809)

0x60c0001d7700 is located 0 bytes inside of 128-byte region
[0x60c0001d7700,0x60c0001d7780)
freed by thread T0 here:
    #0 0x7fb5dfbf97a8 in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xde7a8)
    #1 0x556ecf725656 in nasm_free nasmlib/alloc.c:108
    #2 0x556ecf769767 in pp_tokline asm/preproc.c:6750
    #3 0x556ecf76a802 in pp_getline asm/preproc.c:6922
    #4 0x556ecf7231dc in assemble_file asm/nasm.c:1718
    #5 0x556ecf71e567 in main asm/nasm.c:714
    #6 0x7fb5df74bb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

previously allocated by thread T0 here:
    #0 0x7fb5dfbf9d28 in __interceptor_calloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xded28)
    #1 0x556ecf725572 in nasm_calloc nasmlib/alloc.c:72
    #2 0x556ecf7541d6 in count_mmac_params asm/preproc.c:2443
    #3 0x556ecf765d08 in is_mmacro asm/preproc.c:6004
    #4 0x556ecf76722b in expand_mmacro asm/preproc.c:6284
    #5 0x556ecf76a766 in pp_tokline asm/preproc.c:6910
    #6 0x556ecf76a802 in pp_getline asm/preproc.c:6922
    #7 0x556ecf7231dc in assemble_file asm/nasm.c:1718
    #8 0x556ecf71e567 in main asm/nasm.c:714
    #9 0x7fb5df74bb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: double-free (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xde7a8) in __interceptor_free
==32583==ABORTING
```

This is found by Agency for Defense Development (ADD).

Cyrill Gorcunov 2020-08-17 11:32:47 PDT Comment 1

Fixed in 8806c3ca007b84accac21dd88b900fb03614ceb7. Thanks for report!
Actually we've a bunch of memory leaks but this is less destructive than double
free.

Still we need more precise look into our preproc code, sigh...

Cyrill Gorcunov 2020-08-18 06:44:47 PDT Comment 2

*** ~~Bug 3392671~~ has been marked as a duplicate of this bug. ***

Cyrill Gorcunov 2020-08-18 06:45:32 PDT Comment 3

*** ~~Bug 3392670~~ has been marked as a duplicate of this bug. ***