Out-of-bound write in function parse_command_modifiers in vim/vim

0

Valid Reported on Jun 27th 2022

Description

Out-of-bounds write in function `parse_command_modifiers` at ex_docmd.c:3123

Version

```
commit c101abff4c6756db4f5e740fde289decb9452efa (HEAD -> master, tag: v8.2.
```

Proof of Concept

```
guest@elk:~/trung$ ./vim3/src/vim  -u NONE -i NONE -n -m -X -Z -e -s -S ./p
==================================================================
==26557==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000
WRITE of size 7 at 0x602000007f17 thread T0
    #0 0x7f58a13e6779  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79779)
    #1 0x55b4aa3a571d in parse_command_modifiers /home/guest/trung/vim3/src
    #2 0x55b4aa39cc28 in do_one_cmd /home/guest/trung/vim3/src/ex_docmd.c:1
    #3 0x55b4aa398b4f in do_cmdline /home/guest/trung/vim3/src/ex_docmd.c:9
    #4 0x55b4aa54b7e5 in nv_colon /home/guest/trung/vim3/src/normal.c:3200
    #5 0x55b4aa53e53b in normal_cmd /home/guest/trung/vim3/src/normal.c:939
    #6 0x55b4aa3c584c in exec_normal /home/guest/trung/vim3/src/ex_docmd.c:
    #7 0x55b4aa3c5628 in exec_normal_cmd /home/guest/trung/vim3/src/ex_docm
    #8 0x55b4aa3c4ec9 in ex_normal /home/guest/trung/vim3/src/ex_docmd.c:86
    #9 0x55b4aa3a17c9 in do_one_cmd /home/guest/trung/vim3/src/ex_docmd.c:2
    #10 0x55b4aa398b4f in do_cmdline /home/guest/trung/vim3/
    #11 0x55b4aa6b9b28 in do_source_ext /home/guest/trung/v
    #12 0x55b4aa6bac6a in do_source /home/guest/trung/vim3/src/scriptfile.c
```

```
    #13 0x55b4aa6b77a3 in cmd_source /home/guest/trung/vim3/src/scriptfile.
    #14 0x55b4aa6b7804 in ex_source /home/guest/trung/vim3/src/scriptfile.c
    #15 0x55b4aa3a17c9 in do_one_cmd /home/guest/trung/vim3/src/ex_docmd.c:

    #16 0x55b4aa398b4f in do_cmdline /home/guest/trung/vim3/src/ex_docmd.c:
    #17 0x55b4aa396f4e in do_cmdline_cmd /home/guest/trung/vim3/src/ex_docm
    #18 0x55b4aa987cc6 in exe_commands /home/guest/trung/vim3/src/main.c:31
    #19 0x55b4aa980ebb in vim_main2 /home/guest/trung/vim3/src/main.c:780
    #20 0x55b4aa980777 in main /home/guest/trung/vim3/src/main.c:432
    #21 0x7f58a05c9c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #22 0x55b4aa222a99 in _start (/home/guest/trung/vim3/src/vim+0x137a99)

0x602000007f17 is located 0 bytes to the right of 7-byte region [0x60200000
allocated by thread T0 here:
    #0 0x7f58a144bb40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/li
    #1 0x55b4aa222edf in lalloc /home/guest/trung/vim3/src/alloc.c:246
    #2 0x55b4aa222ce4 in alloc /home/guest/trung/vim3/src/alloc.c:151
    #3 0x55b4aa74b7ac in vim_strsave /home/guest/trung/vim3/src/strings.c:2
    #4 0x55b4aa3eccf2 in open_cmdwin /home/guest/trung/vim3/src/ex_getln.c:
    #5 0x55b4aa3e1b76 in getcmdline_int /home/guest/trung/vim3/src/ex_getln
    #6 0x55b4aa3dfb25 in getcmdline /home/guest/trung/vim3/src/ex_getln.c:1
    #7 0x55b4aa3e5865 in getexline /home/guest/trung/vim3/src/ex_getln.c:28
    #8 0x55b4aa3982dd in do_cmdline /home/guest/trung/vim3/src/ex_docmd.c:8
    #9 0x55b4aa54b7e5 in nv_colon /home/guest/trung/vim3/src/normal.c:3200
    #10 0x55b4aa53e53b in normal_cmd /home/guest/trung/vim3/src/normal.c:93
    #11 0x55b4aa3c584c in exec_normal /home/guest/trung/vim3/src/ex_docmd.c
    #12 0x55b4aa3c5628 in exec_normal_cmd /home/guest/trung/vim3/src/ex_doc
    #13 0x55b4aa3c4ec9 in ex_normal /home/guest/trung/vim3/src/ex_docmd.c:8
    #14 0x55b4aa3a17c9 in do_one_cmd /home/guest/trung/vim3/src/ex_docmd.c:
    #15 0x55b4aa398b4f in do_cmdline /home/guest/trung/vim3/src/ex_docmd.c:
    #16 0x55b4aa6b9b28 in do_source_ext /home/guest/trung/vim3/src/scriptfi
    #17 0x55b4aa6bac6a in do_source /home/guest/trung/vim3/src/scriptfile.c
    #18 0x55b4aa6b77a3 in cmd_source /home/guest/trung/vim3/src/scriptfile.
    #19 0x55b4aa6b7804 in ex_source /home/guest/trung/vim3/src/scriptfile.c
    #20 0x55b4aa3a17c9 in do_one_cmd /home/guest/trung/vim3/src/ex_docmd.c:
    #21 0x55b4aa398b4f in do_cmdline /home/guest/trung/vim3/src/ex_docmd.c:
    #22 0x55b4aa396f4e in do_cmdline_cmd /home/guest/trung/vim3/src/ex_docm
    #23 0x55b4aa987cc6 in exe_commands /home/guest/trung/vim3/src/main.c:31
    #24 0x55b4aa980ebb in vim_main2 /home/guest/trung/vim3/src/main.c:780
    #25 0x55b4aa980777 in main /home/guest/trung/vim3/src/main.c:432
    #26 0x7f58a05c9c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-gnu/
Shadow bytes around the buggy address:

  0x0c047fff8f90: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c047fff8fa0: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c047fff8fb0: fa fa fd fa fa fa fd fa fa fa 02 fa fa fa 00 fa
  0x0c047fff8fc0: fa fa 02 fa fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c047fff8fd0: fa fa 02 fa fa fa fd fa fa fa fd fa fa fa 05 fa
=>0x0c047fff8fe0: fa fa[07]fa fa fa 00 04 fa fa 01 fa fa fa 01 fa
  0x0c047fff8ff0: fa fa 01 fa fa fa 01 fa fa fa 07 fa fa fa 03 fa
  0x0c047fff9000: fa fa 00 06 fa fa 00 04 fa fa 01 fa fa fa 01 fa
  0x0c047fff9010: fa fa 03 fa fa fa 01 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff9020: fa fa 01 fa fa fa 01 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff9030: fa fa 02 fa fa fa fd fa fa fa fd fa fa fa fd fa
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
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==26557==ABORTING
```

Attachment

poc4min

Impact

Typically, this can result in corruption of data, a crash, or code execution.

Occurrences

C ex_docmd.c L3123

CVE
CVE-2022-2288
(Published)

Vulnerability Type
CWE-787: Out-of-bounds Write

Severity
High (7.8)

Registry
Other

Affected Version
8.2.5164

Visibility
Public

Status
Fixed

Found by
xikhud
@acquykhud
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 710 times.

We are processing your report and will contact the **vim** team within 24 hours. 5 months ago

We have contacted a member of the **vim** team and are waiting to hear back 5 months ago

We have sent a follow up to the **vim** team. We will try again in 7 days. 5 months ago

Bram Moolenaar 5 months ago Maintainer

Well, this turned out to be tricky to reproduce, but I could see the mistake in the code from the stack trace.

Bram Moolenaar validated this vulnerability 5 months ago

xikhud has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 5 months ago Maintainer

Fixed with patch 9.0.0025

Bram Moolenaar marked this as fixed in **9.0** with commit **c6fdb1** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

ex_docmd.c#L3123 has been validated ✔

Sign in to join this conversation

Chat with us