huntr

Buffer Over-read in function find_next_quote in vim/vim

0

✓ Valid Reported on May 8th 2022

Description

Buffer Over-read in function find_next_quote at textobject.c:1663

POC

```
./vim -u NONE -X -Z -e -s -S ./poc_h4_s.dat -c :qa!
=================================================================
==1740874==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020
READ of size 1 at 0x60200000741a thread T0
    #0 0x10f50eb in find_next_quote /home/fuzz/vim/vim/src/textobject.c:166
    #1 0x10f34a0 in current_quote /home/fuzz/vim/vim/src/textobject.c:1887
    #2 0xb91bb7 in nv_object /home/fuzz/vim/vim/src/normal.c:7094:10
    #3 0xb73831 in nv_edit /home/fuzz/vim/vim/src/normal.c:6873:2
    #4 0xb47473 in normal_cmd /home/fuzz/vim/vim/src/normal.c:930:5
    #5 0x82fb0e in exec_normal /home/fuzz/vim/vim/src/ex_docmd.c:8757:6
    #6 0x82f338 in exec_normal_cmd /home/fuzz/vim/vim/src/ex_docmd.c:8720:5
    #7 0x82eee9 in ex_normal /home/fuzz/vim/vim/src/ex_docmd.c:8638:6
    #8 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #9 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #10 0x1187b5f in call_user_func /home/fuzz/vim/vim/src/userfunc.c:2896
    #11 0x1183c3d in call_user_func_check /home/fuzz/vim/vim/src/userfunc.c
    #12 0x117dfc4 in call_func /home/fuzz/vim/vim/src/userfunc.c:3608:11
    #13 0x117b36f in get_func_tv /home/fuzz/vim/vim/src/userfunc.c:1829:8
    #14 0x11adba6 in ex_call /home/fuzz/vim/vim/src/userfunc.c:5509:6
    #15 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #16 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #17 0x1187b5f in call_user_func /home/fuzz/vim/vim/src/userfunc.c:2896
    #18 0x1183c3d in call_user_func_check /home/fuzz/vim/vir
    #19 0x117dfc4 in call_func /home/fuzz/vim/vim/src/userf
    #20 0x117b36f in get_func_tv /home/fuzz/vim/vim/src/userfunc.c:1829:8
    #21 0x11adba6 in ex_call /home/fuzz/vim/vim/src/userfunc.c:5509:6
    #22 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #23 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17

    #24 0xe8b02c in do_source_ext /home/fuzz/vim/vim/src/scriptfile.c:1674:
    #25 0xe87a86 in do_source /home/fuzz/vim/vim/src/scriptfile.c:1801:12
    #26 0xe873bc in cmd_source /home/fuzz/vim/vim/src/scriptfile.c:1174:14
    #27 0xe86a9e in ex_source /home/fuzz/vim/vim/src/scriptfile.c:1200:2
    #28 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #29 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #30 0x7e9f61 in do_cmdline_cmd /home/fuzz/vim/vim/src/ex_docmd.c:586:12
    #31 0x1450f52 in exe_commands /home/fuzz/vim/vim/src/main.c:3108:2
    #32 0x144d0dd in vim_main2 /home/fuzz/vim/vim/src/main.c:780:2
    #33 0x1442334 in main /home/fuzz/vim/vim/src/main.c:432:12
    #34 0x7ffff78200b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #35 0x41fe5d in _start (/home/fuzz/fuzz-vim/vim/src/vim+0x41fe5d)

0x60200000741a is located 0 bytes to the right of 10-byte region [0x602000
allocated by thread T0 here:
    #0 0x49b0bd in malloc (/home/fuzz/fuzz-vim/vim/src/vim+0x49b0bd)
    #1 0x4cc79a in lalloc /home/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cc67a in alloc /home/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x54b5f4 in ins_str /home/fuzz/vim/vim/src/change.c:1164:12
    #4 0x6b3960 in insertchar /home/fuzz/vim/vim/src/edit.c:2271:2
    #5 0x6abdf9 in insert_special /home/fuzz/vim/vim/src/edit.c:2056:2
    #6 0x69161d in edit /home/fuzz/vim/vim/src/edit.c:1375:3
    #7 0xb91fbc in invoke_edit /home/fuzz/vim/vim/src/normal.c:7021:9
    #8 0xb75185 in nv_edit /home/fuzz/vim/vim/src/normal.c:6991:2
    #9 0xb47473 in normal_cmd /home/fuzz/vim/vim/src/normal.c:930:5
    #10 0x82fb0e in exec_normal /home/fuzz/vim/vim/src/ex_docmd.c:8757:6
    #11 0x82f338 in exec_normal_cmd /home/fuzz/vim/vim/src/ex_docmd.c:8720:
    #12 0x82eee9 in ex_normal /home/fuzz/vim/vim/src/ex_docmd.c:8638:6
    #13 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #14 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #15 0x1187b5f in call_user_func /home/fuzz/vim/vim/src/userfunc.c:2896:
    #16 0x1183c3d in call_user_func_check /home/fuzz/vim/vim/src/userfunc.c
    #17 0x117dfc4 in call_func /home/fuzz/vim/vim/src/userfunc.c:3608:11
    #18 0x117b36f in get_func_tv /home/fuzz/vim/vim/src/userfunc.c:1829:8
    #19 0x11adba6 in ex_call /home/fuzz/vim/vim/src/userfunc
    #20 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_do
    #21 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #22 0xe8b02c in do_source_ext /home/fuzz/vim/vim/src/scriptfile.c:1674
    #22 0xe8b02c in do_source_ext /home/fuzz/vim/vim/src/scriptfile.c:1674:
    #23 0xe87a86 in do_source /home/fuzz/vim/vim/src/scriptfile.c:1801:12
    #24 0xe873bc in cmd_source /home/fuzz/vim/vim/src/scriptfile.c:1174:14

    #25 0xe86a9e in ex_source /home/fuzz/vim/vim/src/scriptfile.c:1200:2
    #26 0x7f8395 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #27 0x7e5315 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #28 0x7e9f61 in do_cmdline_cmd /home/fuzz/vim/vim/src/ex_docmd.c:586:12
    #29 0x1450f52 in exe_commands /home/fuzz/vim/vim/src/main.c:3108:2

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim/vim/src/text
Shadow bytes around the buggy address:
  0x0c047fff8e30: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8e40: fa fa fd fd fa fa fd fa fa fa 01 fa fa fa 00 00
  0x0c047fff8e50: fa fa 01 fa fa fa fd fa fa fa fd fd fa fa fd fd
  0x0c047fff8e60: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8e70: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
=>0x0c047fff8e80: fa fa 00[02]fa fa 00 05 fa fa fd fa fa fa 00 03
  0x0c047fff8e90: fa fa 02 fa fa fa 00 04 fa fa 01 fa fa fa 05 fa
  0x0c047fff8ea0: fa fa 00 04 fa fa 01 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff8eb0: fa fa 01 fa fa fa 07 fa fa fa 03 fa fa fa 00 06
  0x0c047fff8ec0: fa fa 00 04 fa fa 01 fa fa fa 01 fa fa fa 03 fa
  0x0c047fff8ed0: fa fa 01 fa fa fa 01 fa fa fa 01 fa fa fa 01 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
```

```
    Right alloca redzone:     cb
    Shadow gap:               cc


  ==1740874==ABORTING
```

poc_h4_s.dat

Impact

This vulnerabilities are capable of crashing software, Modify Memory, and possible remote execution

CVE
CVE-2022-1629
(Published)

Vulnerability Type
CWE-126: Buffer Over-read

Severity
Medium (6.6)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,110 times.

We are processing your report and will contact the **vim** team within 24 hours. 7 months ago

We have contacted a member of the **vim** team and are waiting to hear back 7 months ago

Bram Moolenaar validated this vulnerability 7 months ago

I can reproduce the problem.

TDHX ICS Security has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar marked this as fixed in **8.2** with commit **53a702** 7 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Bram Moolenaar 7 months ago

Fixed in patch 8.2.4925

Sign in to join this conversation

Chat with us