Use After Free in function find_pattern_in_path in vim/vim

0

Valid Reported on May 25th 2022

Description

Use After Free in function find_pattern_in_path at search.c:3653

vim version

```
git log
commit 4c3d21acaa09d929e6afe10288babe1d0af3de35 (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /mnt/share/max/fuzz/poc/vim/poc_
==================================================================
==2466037==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000
READ of size 1 at 0x602000007d70 thread T0
    #0 0x431c9e in strncmp (/home/fuzz/fuzz-vim/vim/src/vim+0x431c9e)
    #1 0xe8a896 in find_pattern_in_path /home/fuzz/fuzz/vim/vim/src/search.
    #2 0xb54726 in nv_brackets /home/fuzz/fuzz/vim/vim/src/normal.c:4460:6
    #3 0xb1ffe1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #4 0x813dfe in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:
    #5 0x813628 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8
    #6 0x8131d9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #7 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #8 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #9 0xe57b3c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1
    #10 0xe54596 in do_source /home/fuzz/fuzz/vim/vim/src/s
    #11 0xe53ecc in cmd_source /home/fuzz/fuzz/vim/vim/src/s
    #12 0xe535ae in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
```

```
    #13 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #14 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #15 0x7cdcf1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #16 0x1423d62 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #17 0x141fefb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #18 0x14155f5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #19 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #20 0x41ea6d in _start (/home/fuzz/fuzz-vim/vim/src/vim+0x41ea6d)

0x602000007d70 is located 0 bytes inside of 2-byte region [0x602000007d70,0
freed by thread T0 here:
    #0 0x499a62 in free (/home/fuzz/fuzz-vim/vim/src/vim+0x499a62)
    #1 0x4cbe06 in vim_free /home/fuzz/fuzz/vim/vim/src/alloc.c:621:2
    #2 0xa648a5 in ml_flush_line /home/fuzz/fuzz/vim/vim/src/memline.c:406
    #3 0xa7a0a5 in ml_get_buf /home/fuzz/fuzz/vim/vim/src/memline.c:2651:2
    #4 0xa76209 in ml_get /home/fuzz/fuzz/vim/vim/src/memline.c:2564:12
    #5 0xe87ef3 in find_pattern_in_path /home/fuzz/fuzz/vim/vim/src/search.
    #6 0xb54726 in nv_brackets /home/fuzz/fuzz/vim/vim/src/normal.c:4460:6
    #7 0xb1ffe1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #8 0x813dfe in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762
    #9 0x813628 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8
    #10 0x8131d9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #11 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #12 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #13 0xe57b3c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #14 0xe54596 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #15 0xe53ecc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #16 0xe535ae in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #17 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #18 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #19 0x7cdcf1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #20 0x1423d62 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #21 0x141fefb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #22 0x14155f5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #23 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

previously allocated by thread T0 here:
    #0 0x499ccd in malloc (/home/fuzz/fuzz-vim/vim/src/vim+0
    #1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc
    #2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
```

```
    #3 0x54c95d in ins_char_bytes /home/fuzz/fuzz/vim/vim/src/change.c:1095
    #4 0x54d63b in ins_char /home/fuzz/fuzz/vim/vim/src/change.c:1010:5
    #5 0x69654f in insertchar /home/fuzz/fuzz/vim/vim/src/edit.c:2277:6

    #6 0x68e5e9 in insert_special /home/fuzz/fuzz/vim/vim/src/edit.c:2040:2
    #7 0x673dd7 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1361:3
    #8 0xb6a68c in invoke_edit /home/fuzz/fuzz/vim/vim/src/normal.c:7028:9
    #9 0xb6c3a4 in n_opencmd /home/fuzz/fuzz/vim/vim/src/normal.c:6275:6
    #10 0xb52b56 in nv_open /home/fuzz/fuzz/vim/vim/src/normal.c:7409:2
    #11 0xb1ffe1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #12 0x813dfe in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762
    #13 0x813628 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:
    #14 0x8131d9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #15 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
    #16 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #17 0xe57b3c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #18 0xe54596 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #19 0xe53ecc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #20 0xe535ae in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #21 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
    #22 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #23 0x7cdcf1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #24 0x1423d62 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #25 0x141fefb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #26 0x14155f5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #27 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free (/home/fuzz/fuzz-vim/vim/src
Shadow bytes around the buggy address:
  0x0c047fff8f50: fa fa fd fd fa fa fd fd fa fa fd fa fa fa fd fd
  0x0c047fff8f60: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fa
  0x0c047fff8f70: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fa
  0x0c047fff8f80: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8f90: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fa
=>0x0c047fff8fa0: fa fa 01 fa fa fa 00 00 fa fa 01 fa fa fa[fd]fa
  0x0c047fff8fb0: fa fa 05 fa fa fa 02 fa fa fa 01 fa fa fa 00 00
  0x0c047fff8fc0: fa fa 00 07 fa fa 06 fa fa fa 06 fa fa fa 06 fa
  0x0c047fff8fd0: fa fa 01 fa fa fa 01 fa fa fa 06 fa fa fa 01 fa
  0x0c047fff8fe0: fa fa 01 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8ff0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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
  Shadow gap:              cc
==2466037==ABORTING
```

poc_h16_s.dat

Impact

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

CVE
CVE-2022-1898
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,157 times.

We are processing your report and will contact the **vim** team within 24 hours. 6 months ago

We have contacted a member of the **vim** team and are waiting to hear back 6 months ago

Bram Moolenaar validated this vulnerability 6 months ago

Similar to what was fixed by Patch 8.2.4979

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 6 months ago

Fixed with patch 8.2.5024

Bram Moolenaar marked this as fixed in 8.2 with commit e2fa21 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation