Use After Free in function process_next_cpt_value in vim/vim

0

Valid Reported on Sep 21st 2022

Description

Use After Free in function process_next_cpt_value at insexpand.c:3227.

vim version

```
git log
commit 5c645a25bb8e6d766db720a44b9ceeff39d1e92b (HEAD -> master, tag: v9.0.
```

Proof of Concept

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/fuzz/test/poc11_huaf.dat -
==================================================================
==38955==ERROR: AddressSanitizer: heap-use-after-free on address 0x6020000(
READ of size 1 at 0x60200000049a thread T0
    #0 0x558ba0c60f80 in process_next_cpt_value /home/fuzz/vim/src/insexpar
    #1 0x558ba0c64b7a in ins_compl_get_exp /home/fuzz/vim/src/insexpand.c:3
    #2 0x558ba0c65876 in find_next_completion_match /home/fuzz/vim/src/inse
    #3 0x558ba0c65c43 in ins_compl_next /home/fuzz/vim/src/insexpand.c:4136
    #4 0x558ba0c68d69 in ins_complete /home/fuzz/vim/src/insexpand.c:4987
    #5 0x558ba0abe0b9 in edit /home/fuzz/vim/src/edit.c:1286
    #6 0x558ba0d38577 in invoke_edit /home/fuzz/vim/src/normal.c:7049
    #7 0x558ba0d383bf in nv_edit /home/fuzz/vim/src/normal.c:7019
    #8 0x558ba0d10b02 in normal_cmd /home/fuzz/vim/src/normal.c:937
    #9 0x558ba0b91cfb in exec_normal /home/fuzz/vim/src/ex_d
    #10 0x558ba0b91aba in exec_normal_cmd /home/fuzz/vim/sr
    #11 0x558ba0b9135e in ex_normal /home/fuzz/vim/src/ex_docmd.c:8728
```

```
    #12 0x558ba0b6d76e in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #13 0x558ba0b649ca in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #14 0x558ba0e8a865 in do_source_ext /home/fuzz/vim/src/scriptfile.c:166

    #15 0x558ba0e8ba9a in do_source /home/fuzz/vim/src/scriptfile.c:1811
    #16 0x558ba0e88558 in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #17 0x558ba0e885bd in ex_source /home/fuzz/vim/src/scriptfile.c:1189
    #18 0x558ba0b6d76e in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #19 0x558ba0b649ca in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #20 0x558ba0b62d64 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #21 0x558ba116d0d1 in exe_commands /home/fuzz/vim/src/main.c:3139
    #22 0x558ba116623a in vim_main2 /home/fuzz/vim/src/main.c:781
    #23 0x558ba1165af2 in main /home/fuzz/vim/src/main.c:432
    #24 0x7f3b36f22082 in __libc_start_main ../csu/libc-start.c:308
    #25 0x558ba09e0e4d in _start (/home/fuzz/vim/src/vim+0x13be4d)

0x60200000049a is located 10 bytes inside of 12-byte region [0x602000000490
freed by thread T0 here:
    #0 0x7f3b373b940f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x558ba09e1576 in vim_free /home/fuzz/vim/src/alloc.c:623
    #2 0x558ba0d85cbe in clear_string_option /home/fuzz/vim/src/optionstr.c
    #3 0x558ba0a0816c in free_buf_options /home/fuzz/vim/src/buffer.c:2337
    #4 0x558ba0d7810b in buf_copy_options /home/fuzz/vim/src/option.c:5920
    #5 0x558ba0a06f38 in buflist_new /home/fuzz/vim/src/buffer.c:2129
    #6 0x558ba0b4f27f in do_ecmd /home/fuzz/vim/src/ex_cmds.c:2663
    #7 0x558ba0a024b7 in empty_curbuf /home/fuzz/vim/src/buffer.c:1210
    #8 0x558ba0a030d1 in do_buffer_ext /home/fuzz/vim/src/buffer.c:1394
    #9 0x558ba0a0439f in do_buffer /home/fuzz/vim/src/buffer.c:1588
    #10 0x558ba0a044ac in do_bufdel /home/fuzz/vim/src/buffer.c:1622
    #11 0x558ba0b81966 in ex_bunload /home/fuzz/vim/src/ex_docmd.c:5525
    #12 0x558ba0b6d76e in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #13 0x558ba0b649ca in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #14 0x558ba100a337 in call_user_func /home/fuzz/vim/src/userfunc.c:2944
    #15 0x558ba100b5a0 in call_user_func_check /home/fuzz/vim/src/userfunc.
    #16 0x558ba100de4b in call_func /home/fuzz/vim/src/userfunc.c:3662
    #17 0x558ba100c6eb in call_callback /home/fuzz/vim/src/userfunc.c:3407
    #18 0x558ba0f561cb in find_tagfunc_tags /home/fuzz/vim/src/tag.c:1480
    #19 0x558ba0f5804b in findtags_apply_tfu /home/fuzz/vim/src/tag.c:1847
    #20 0x558ba0f5fd20 in find_tags /home/fuzz/vim/src/tag.c:2155
    #21 0x558ba0c624b4 in get_next_tag_completion /home/fuz
    #22 0x558ba0c646a4 in get_next_completion_match /home/fuzz/vim/src/inse
```

```
    #23 0x558ba0c64bf4 in ins_compl_get_exp /home/fuzz/vim/src/insexpand.c:
    #24 0x558ba0c65876 in find_next_completion_match /home/fuzz/vim/src/ins
    #25 0x558ba0c65c43 in ins_compl_next /home/fuzz/vim/src/insexpand.c:413

    #26 0x558ba0c68d69 in ins_complete /home/fuzz/vim/src/insexpand.c:4987
    #27 0x558ba0abe0b9 in edit /home/fuzz/vim/src/edit.c:1286
    #28 0x558ba0d38577 in invoke_edit /home/fuzz/vim/src/normal.c:7049
    #29 0x558ba0d383bf in nv_edit /home/fuzz/vim/src/normal.c:7019

previously allocated by thread T0 here:
    #0 0x7f3b373b9808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x558ba09e128a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x558ba09e107b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x558ba0f1e19c in vim_strsave /home/fuzz/vim/src/strings.c:27
    #4 0x558ba0d85fca in set_string_option_direct /home/fuzz/vim/src/option
    #5 0x558ba0d5cfd1 in set_option_default /home/fuzz/vim/src/option.c:574
    #6 0x558ba0d5d86a in set_options_default /home/fuzz/vim/src/option.c:65
    #7 0x558ba0d5c1d9 in set_init_1 /home/fuzz/vim/src/option.c:297
    #8 0x558ba11665f3 in common_init /home/fuzz/vim/src/main.c:991
    #9 0x558ba1165800 in main /home/fuzz/vim/src/main.c:185
    #10 0x7f3b36f22082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/vim/src/insexpand
Shadow bytes around the buggy address:
  0x0c047fff8040: fa fa 00 03 fa fa 00 02 fa fa fd fa fa fa 07 fa
  0x0c047fff8050: fa fa fd fa fa fa 04 fa fa fa fd fa fa fa 01 fa
  0x0c047fff8060: fa fa 01 fa fa fa 01 fa fa fa fd fa fa fa 01 fa
  0x0c047fff8070: fa fa fd fa fa fa 01 fa fa fa fd fa fa fa 01 fa
  0x0c047fff8080: fa fa 01 fa fa fa 01 fa fa fa fd fa fa fa 07 fa
=>0x0c047fff8090: fa fa fd[fd]fa fa 00 04 fa fa 01 fa fa fa 01 fa
  0x0c047fff80a0: fa fa fd fa fa fa 01 fa fa fa fd fd fa fa 00 02
  0x0c047fff80b0: fa fa 05 fa fa fa 05 fa fa fa fd fd fa fa 00 07
  0x0c047fff80c0: fa fa fd fa fa fa 01 fa fa fa fd fa fa fa 01 fa
  0x0c047fff80d0: fa fa fd fa fa fa 01 fa fa fa fd fa fa fa 05 fa
  0x0c047fff80e0: fa fa fd fa fa fa 01 fa fa fa 02 fa fa fa 02 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
  ==38955==ABORTING
```

poc download url: https://github.com/Janette88/vim/blob/main/poc11_huaf.dat

Impact

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

CVE
CVE-2022-3297
(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 1,418 times.

We are processing your report and will contact the **vim** team within 24 hours. 2 months ago

We have contacted a member of the **vim** team and are waiting to hear back 2 months ago

Bram Moolenaar validated this vulnerability 2 months ago

I can reproduce the problem.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 2 months ago Maintainer

Discovered a few more problems while turning the POC into a regression text. Ended up with patch 9.0.0579

Bram Moolenaar marked this as fixed in **9.0.0579** with commit **0ff018** 2 mon

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Sign in to join this conversation