Use After Free in function vim_vsnprintf_typval in vim/vim

0

✓ Valid   Reported on Aug 18th 2022

Description

Use After Free in function vim_vsnprintf_typval at vim/src/strings.c:2299.

vim version

```
git log
commit 9e043181ad51536f23d069e719d6f6b96c4c0ec0 (grafted, HEAD -> master, t
```

Proof of Concept

```
 ./vim -u NONE -X -Z -e -s -S /home/fuzz/test/poc4_huaf.dat -c :qa!
=================================================================
==118758==ERROR: AddressSanitizer: heap-use-after-free on address 0x6020000
READ of size 2 at 0x602000006e50 thread T0
    #0 0x7fb70da36a7c in __interceptor_strlen ../../../../src/libsanitizer/
    #1 0x557b49b9c782 in vim_vsnprintf_typval /home/fuzz/vim/src/strings.c:
    #2 0x557b49b9b646 in vim_vsnprintf /home/fuzz/vim/src/strings.c:2050
    #3 0x557b49de100c in semsg /home/fuzz/vim/src/message.c:812
    #4 0x557b49bc5fdd in do_tag /home/fuzz/vim/src/tag.c:723
    #5 0x557b4980a948 in ex_tag_cmd /home/fuzz/vim/src/ex_docmd.c:9023
    #6 0x557b4980a666 in ex_tag /home/fuzz/vim/src/ex_docmd.c:8974
    #7 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #8 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #9 0x557b497daba1 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #10 0x557b49c188ff in f_assert_fails /home/fuzz/vim/src/testing.c:618
    #11 0x557b4977b390 in call_internal_func /home/fuzz/vim
    #12 0x557b49c81108 in call_func /home/fuzz/vim/src/userfunc.c:3617
    #13 0x557b49c779fa in get_func_tv /home/fuzz/vim/src/userfunc.c:1819
    #14 0x557b49c8d5d1 in ex_call /home/fuzz/vim/src/userfunc.c:5578
    #15 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #16 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #17 0x557b49aff98c in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #18 0x557b49b00abe in do_source /home/fuzz/vim/src/scriptfile.c:1803
    #19 0x557b49afd626 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #20 0x557b49afd68b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #21 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #22 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #23 0x557b497daba1 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #24 0x557b49dd7093 in exe_commands /home/fuzz/vim/src/main.c:3133
    #25 0x557b49dd0201 in vim_main2 /home/fuzz/vim/src/main.c:780
    #26 0x557b49dcfab9 in main /home/fuzz/vim/src/main.c:432
    #27 0x7fb70d645082 in __libc_start_main ../csu/libc-start.c:308
    #28 0x557b4965be4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x602000006e50 is located 0 bytes inside of 2-byte region [0x602000006e50,0
freed by thread T0 here:
    #0 0x7fb70dadc40f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x557b4965c53a in vim_free /home/fuzz/vim/src/alloc.c:625
    #2 0x557b49d372ec in win_free /home/fuzz/vim/src/window.c:5212
    #3 0x557b49d2d21b in win_free_mem /home/fuzz/vim/src/window.c:2942
    #4 0x557b49d2b98f in win_close /home/fuzz/vim/src/window.c:2678
    #5 0x557b4967d43d in do_buffer_ext /home/fuzz/vim/src/buffer.c:1400
    #6 0x557b4967e6c6 in do_buffer /home/fuzz/vim/src/buffer.c:1598
    #7 0x557b4967e7d3 in do_bufdel /home/fuzz/vim/src/buffer.c:1632
    #8 0x557b497f9478 in ex_bunload /home/fuzz/vim/src/ex_docmd.c:5502
    #9 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #10 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #11 0x557b49c7d4fd in call_user_func /home/fuzz/vim/src/userfunc.c:2886
    #12 0x557b49c7e74b in call_user_func_check /home/fuzz/vim/src/userfunc.
    #13 0x557b49c80fff in call_func /home/fuzz/vim/src/userfunc.c:3599
    #14 0x557b49c7f891 in call_callback /home/fuzz/vim/src/userfunc.c:3344
    #15 0x557b49bca5d2 in find_tagfunc_tags /home/fuzz/vim/src/tag.c:1463
    #16 0x557b49bcc452 in findtags_apply_tfu /home/fuzz/vim/src/tag.c:1830
    #17 0x557b49bd4127 in find_tags /home/fuzz/vim/src/tag.c:3138
    #18 0x557b49bc5aca in do_tag /home/fuzz/vim/src/tag.c:681
    #19 0x557b4980a948 in ex_tag_cmd /home/fuzz/vim/src/ex_d
    #20 0x557b4980a666 in ex_tag /home/fuzz/vim/src/ex_docm
    #21 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #22 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #23 0x557b497daba1 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #24 0x557b49c188ff in f_assert_fails /home/fuzz/vim/src/testing.c:618

    #25 0x557b4977b390 in call_internal_func /home/fuzz/vim/src/evalfunc.c:
    #26 0x557b49c81108 in call_func /home/fuzz/vim/src/userfunc.c:3617
    #27 0x557b49c779fa in get_func_tv /home/fuzz/vim/src/userfunc.c:1819
    #28 0x557b49c8d5d1 in ex_call /home/fuzz/vim/src/userfunc.c:5578
    #29 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570

previously allocated by thread T0 here:
    #0 0x7fb70dadc808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x557b4965c28a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x557b4965c07b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x557b49b92674 in vim_strsave /home/fuzz/vim/src/strings.c:27
    #4 0x557b49bc47df in do_tag /home/fuzz/vim/src/tag.c:403
    #5 0x557b4980a948 in ex_tag_cmd /home/fuzz/vim/src/ex_docmd.c:9023
    #6 0x557b4980a666 in ex_tag /home/fuzz/vim/src/ex_docmd.c:8974
    #7 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #8 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #9 0x557b497daba1 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #10 0x557b49c188ff in f_assert_fails /home/fuzz/vim/src/testing.c:618
    #11 0x557b4977b390 in call_internal_func /home/fuzz/vim/src/evalfunc.c:
    #12 0x557b49c81108 in call_func /home/fuzz/vim/src/userfunc.c:3617
    #13 0x557b49c779fa in get_func_tv /home/fuzz/vim/src/userfunc.c:1819
    #14 0x557b49c8d5d1 in ex_call /home/fuzz/vim/src/userfunc.c:5578
    #15 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #16 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #17 0x557b49aff98c in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #18 0x557b49b00abe in do_source /home/fuzz/vim/src/scriptfile.c:1803
    #19 0x557b49afd626 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #20 0x557b49afd68b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #21 0x557b497e5564 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #22 0x557b497dc807 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #23 0x557b497daba1 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #24 0x557b49dd7093 in exe_commands /home/fuzz/vim/src/main.c:3133
    #25 0x557b49dd0201 in vim_main2 /home/fuzz/vim/src/main.c:780
    #26 0x557b49dcfab9 in main /home/fuzz/vim/src/main.c:432
    #27 0x7fb70d645082 in __libc_start_main ../csu/libc-start

SUMMARY: AddressSanitizer: heap-use-after-free ../../../../src/libsanitizer
```

```
Shadow bytes around the buggy address:
  0x0c047fff8d70: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c047fff8d80: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa

  0x0c047fff8d90: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8da0: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c047fff8db0: fa fa fd fa fa fa fd fa fa fa 00 05 fa fa 04 fa
=>0x0c047fff8dc0: fa fa 00 05 fa fa 04 fa fa fa[fd]fa fa fa 02 fa
  0x0c047fff8dd0: fa fa fd fd fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8de0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8df0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8e00: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c047fff8e10: fa fa fd fd fa fa 00 03 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
==118758==ABORTING
```

<p><a href="https://github.com/Janette88/vim/blob/main/poc4_huaf.dat">poc4_h

Impact

Impact

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

CVE
CVE-2022-2946
(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 997 times.

We are processing your report and will contact the vim team within 24 hours. 3 months ago

Chat with us

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.

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 with patch 9.0.0246

Bram Moolenaar marked this as fixed in 9.0.0245 with commit adce96 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation