huntr

Use After Free in function string_quote in vim/vim

0

✓ Valid Reported on Aug 12th 2022

Description

Use After Free in function string_quote at vim/src/strings.c:777

vim version

```
git log
commit c9b6570fab46bf2c246a954cfb8c0d95fe2746b3 (grafted, HEAD -> master, t
```

Proof of Concept

```
 ./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/fuzz/test/poc1_uaf.dat -c
=================================================================
==60044==ERROR: AddressSanitizer: heap-use-after-free on address 0x60400000
READ of size 2 at 0x604000000250 thread T0
    #0 0x7f3438582a7c in __interceptor_strlen ../../../../src/libsanitizer/
    #1 0x559d5c7889ba in string_quote /home/fuzz/vim/src/strings.c:777
    #2 0x559d5c35cf02 in echo_string_core /home/fuzz/vim/src/eval.c:5470
    #3 0x559d5c83ea0e in tv2string /home/fuzz/vim/src/typval.c:2413
    #4 0x559d5c809fc3 in fill_assert_error /home/fuzz/vim/src/testing.c:23
    #5 0x559d5c80cdac in f_assert_fails /home/fuzz/vim/src/testing.c:730
    #6 0x559d5c36f041 in call_internal_func /home/fuzz/vim/src/evalfunc.c:2
    #7 0x559d5c874b6f in call_func /home/fuzz/vim/src/userfunc.c:3632
    #8 0x559d5c86b461 in get_func_tv /home/fuzz/vim/src/userfunc.c:1834
    #9 0x559d5c88102f in ex_call /home/fuzz/vim/src/userfunc.c:5592
    #10 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #11 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_
    #12 0x559d5c6f340d in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #13 0x559d5c6f453f in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #13 0x559d5c6f453f in do_source /home/fuzz/vim/src/scriptfile.c:1201
    #14 0x559d5c6f10ce in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #15 0x559d5c6f1133 in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #16 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #17 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #18 0x559d5c3ce825 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #19 0x559d5c9ca784 in exe_commands /home/fuzz/vim/src/main.c:3133
    #20 0x559d5c9c38f2 in vim_main2 /home/fuzz/vim/src/main.c:780
    #21 0x559d5c9c31aa in main /home/fuzz/vim/src/main.c:432
    #22 0x7f3438191082 in __libc_start_main ../csu/libc-start.c:308
    #23 0x559d5c24fe4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x604000000250 is located 0 bytes inside of 34-byte region [0x604000000250,
freed by thread T0 here:
    #0 0x7f343862840f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x559d5c25053a in vim_free /home/fuzz/vim/src/alloc.c:625
    #2 0x559d5c832cdd in clear_tv /home/fuzz/vim/src/typval.c:115
    #3 0x559d5c39e5b3 in set_vim_var_string /home/fuzz/vim/src/evalvars.c:2
    #4 0x559d5c9d3e32 in emsg_core /home/fuzz/vim/src/message.c:686
    #5 0x559d5c9d454f in emsg /home/fuzz/vim/src/message.c:785
    #6 0x559d5c6698a5 in seen_endbrace /home/fuzz/vim/src/regexp_bt.c:1228
    #7 0x559d5c6a2ece in nfa_regatom /home/fuzz/vim/src/regexp_nfa.c:1491
    #8 0x559d5c6a6bed in nfa_regpiece /home/fuzz/vim/src/regexp_nfa.c:2152
    #9 0x559d5c6a7adc in nfa_regconcat /home/fuzz/vim/src/regexp_nfa.c:2396
    #10 0x559d5c6a7ba9 in nfa_regbranch /home/fuzz/vim/src/regexp_nfa.c:242
    #11 0x559d5c6a802e in nfa_reg /home/fuzz/vim/src/regexp_nfa.c:2490
    #12 0x559d5c6a8460 in re2post /home/fuzz/vim/src/regexp_nfa.c:2910
    #13 0x559d5c6bbe5b in nfa_regcomp /home/fuzz/vim/src/regexp_nfa.c:7445
    #14 0x559d5c6bc701 in vim_regcomp /home/fuzz/vim/src/regexp.c:2734
    #15 0x559d5c34c39c in pattern_match /home/fuzz/vim/src/eval.c:2053
    #16 0x559d5c80c861 in f_assert_fails /home/fuzz/vim/src/testing.c:666
    #17 0x559d5c36f041 in call_internal_func /home/fuzz/vim/src/evalfunc.c:
    #18 0x559d5c874b6f in call_func /home/fuzz/vim/src/userfunc.c:3632
    #19 0x559d5c86b461 in get_func_tv /home/fuzz/vim/src/userfunc.c:1834
    #20 0x559d5c88102f in ex_call /home/fuzz/vim/src/userfunc.c:5592
    #21 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #22 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #23 0x559d5c6f340d in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #24 0x559d5c6f453f in do_source /home/fuzz/vim/src/scriptfile.c:1201
    #25 0x559d5c6f10ce in cmd_source /home/fuzz/vim/src/scr
    #26 0x559d5c6f1133 in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #27 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #27 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #28 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #29 0x559d5c3ce825 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586


previously allocated by thread T0 here:
    #0 0x7f3438628808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x559d5c25028a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x559d5c25007b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x559d5c7860f5 in vim_strsave /home/fuzz/vim/src/strings.c:27
    #4 0x559d5c39e682 in set_vim_var_string /home/fuzz/vim/src/evalvars.c:2
    #5 0x559d5c9d3e32 in emsg_core /home/fuzz/vim/src/message.c:686
    #6 0x559d5c9d454f in emsg /home/fuzz/vim/src/message.c:785
    #7 0x559d5c3d991b in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2623
    #8 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #9 0x559d5c3ce825 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #10 0x559d5c80c375 in f_assert_fails /home/fuzz/vim/src/testing.c:617
    #11 0x559d5c36f041 in call_internal_func /home/fuzz/vim/src/evalfunc.c:
    #12 0x559d5c874b6f in call_func /home/fuzz/vim/src/userfunc.c:3632
    #13 0x559d5c86b461 in get_func_tv /home/fuzz/vim/src/userfunc.c:1834
    #14 0x559d5c88102f in ex_call /home/fuzz/vim/src/userfunc.c:5592
    #15 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #16 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #17 0x559d5c6f340d in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #18 0x559d5c6f453f in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #19 0x559d5c6f10ce in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #20 0x559d5c6f1133 in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #21 0x559d5c3d91e8 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #22 0x559d5c3d048b in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #23 0x559d5c3ce825 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #24 0x559d5c9ca784 in exe_commands /home/fuzz/vim/src/main.c:3133
    #25 0x559d5c9c38f2 in vim_main2 /home/fuzz/vim/src/main.c:780
    #26 0x559d5c9c31aa in main /home/fuzz/vim/src/main.c:432
    #27 0x7f3438191082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-use-after-free ../../../../src/libsanitizer
Shadow bytes around the buggy address:
  0x0c087fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff8000: fa fa 00 00 00 00 00 04 fa fa 00 00 00 00 00 04
  0x0c087fff8010: fa fa 00 00 00 00 02 fa fa fa fd fd fd fd
  0x0c087fff8020: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 fa
  0x0c087fff8030: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 01 fa
  0x0c087fff8030: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 01 fa
=>0x0c087fff8040: fa fa 00 00 00 00 02 fa fa fa[fd]fd fd fd fd fa
  0x0c087fff8050: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 02 fa

  0x0c087fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8090: 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
==60044==ABORTING
```

<p><a href="https://github.com/Janette88/vim/blob/main/poc1_uaf.dat">poc1_uaf.dat</a></p>

Impact

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

CVE

CVE-2022-2817
(Published)

Vulnerability Type

CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Affected Version
<=v9.0.0203

Visibility
Public

Status
Fixed

Found by

janette88

@janette88

master

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 810 times.

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

janette88 modified the report 3 months ago

janette88 modified the report 3 months ago

We have contacted a member of the vim team and are waiting to hear bac

Chat with us

janette88 modified the report 3 months ago janette88 modified the report 3 months ago

janette88 3 months ago Researcher

i submitted another report which belonged to "use after free" . The system poped up a hint : edit origin report . i 've thought maybe it used the same template and would appended a new report .After i edited , it deleted origin report i submitted the day before yesterday:(how can i submitted a new report with the same type ?

janette88 3 months ago Researcher

maybe the new bug report covered the old one . Now i recovered the origin report and then tried to sent another report again . i don't know how to send the same type bug without hint. It always poped up "edited origin report".

janette88 modified the report 3 months ago

Bram Moolenaar validated this vulnerability 3 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 3 months ago Maintainer

Fixed with patch 9.0.0213

Bram Moolenaar marked this as fixed in 9.0.0212 with commit 249e1b 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation