Heap Use After Free in function skipwhite in vim/vim

0

Valid Reported on Jul 5th 2022

Description

Heap Use After Free in function skipwhite at charset.c:1428

vim version

```
git log
commit 324478037923feef1eb8a771648e38ade9e5e05a (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_huaf4_s.dat -c :qa
==================================================================
==10794==ERROR: AddressSanitizer: heap-use-after-free on address 0x60300000
READ of size 1 at 0x603000000d95 thread T0
    #0 0x14039ad in skipwhite /home/fuzz/fuzz/vim/afl/src/charset.c:1428:12
    #1 0x1150ed1 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:1859
    #2 0x6e5380 in eval_func /home/fuzz/fuzz/vim/afl/src/eval.c:2113:8
    #3 0x6e34ee in eval9 /home/fuzz/fuzz/vim/afl/src/eval.c:4033:9
    #4 0x6ef209 in eval8 /home/fuzz/fuzz/vim/afl/src/eval.c:3602:11
    #5 0x6ecff8 in eval7 /home/fuzz/fuzz/vim/afl/src/eval.c:3394:9
    #6 0x6e9f4f in eval6 /home/fuzz/fuzz/vim/afl/src/eval.c:3157:9
    #7 0x6e8aa2 in eval5 /home/fuzz/fuzz/vim/afl/src/eval.c:3046:9
    #8 0x6e729c in eval4 /home/fuzz/fuzz/vim/afl/src/eval.c:2897:9
    #9 0x6e599f in eval3 /home/fuzz/fuzz/vim/afl/src/eval.c:2758:9
    #10 0x6c138f in eval2 /home/fuzz/fuzz/vim/afl/src/eval.
    #11 0x6a327f in eval1 /home/fuzz/fuzz/vim/afl/src/eval.c:
    #12 0x6c01d5 in eval0 retarg /home/fuzz/fuzz/vim/afl/src/eval.c:2389:11
```

```
#13 0x6a0817 in eval0 /home/fuzz/fuzz/vim/afl/src/eval.c:2364:12
#14 0x6a7475 in eval_to_string_eap /home/fuzz/fuzz/vim/afl/src/eval.c:5
#15 0x6a761f in eval_to_string /home/fuzz/fuzz/vim/afl/src/eval.c:541:1
#16 0xcefa73 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:26
#17 0xcf3b2b in vim_regsub_multi /home/fuzz/fuzz/vim/afl/src/regexp.c:1
#18 0x7b3ed8 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:442
#19 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#20 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#21 0x115d2ac in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#22 0x115939d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/userf
#23 0x1153744 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3614:
#24 0x1150ae3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#25 0x6e5380 in eval_func /home/fuzz/fuzz/vim/afl/src/eval.c:2113:8
#26 0x6e34ee in eval9 /home/fuzz/fuzz/vim/afl/src/eval.c:4033:9
#27 0x6ef209 in eval8 /home/fuzz/fuzz/vim/afl/src/eval.c:3602:11
#28 0x6ecff8 in eval7 /home/fuzz/fuzz/vim/afl/src/eval.c:3394:9
#29 0x6e9f4f in eval6 /home/fuzz/fuzz/vim/afl/src/eval.c:3157:9
#30 0x6e8aa2 in eval5 /home/fuzz/fuzz/vim/afl/src/eval.c:3046:9
#31 0x6e729c in eval4 /home/fuzz/fuzz/vim/afl/src/eval.c:2897:9
#32 0x6e599f in eval3 /home/fuzz/fuzz/vim/afl/src/eval.c:2758:9
#33 0x6c138f in eval2 /home/fuzz/fuzz/vim/afl/src/eval.c:2632:9
#34 0x6a327f in eval1 /home/fuzz/fuzz/vim/afl/src/eval.c:2478:9
#35 0x6c01d5 in eval0_retarg /home/fuzz/fuzz/vim/afl/src/eval.c:2389:11
#36 0x6a0817 in eval0 /home/fuzz/fuzz/vim/afl/src/eval.c:2364:12
#37 0x6a7475 in eval_to_string_eap /home/fuzz/fuzz/vim/afl/src/eval.c:5
#38 0x6a761f in eval_to_string /home/fuzz/fuzz/vim/afl/src/eval.c:541:1
#39 0xcefa73 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:26
#40 0xcf3b2b in vim_regsub_multi /home/fuzz/fuzz/vim/afl/src/regexp.c:1
#41 0x7b3ed8 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:442
#42 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#43 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#44 0x115d2ac in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#45 0x115939d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/userf
#46 0x1153744 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3614:
#47 0x1150ae3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#48 0x6e5380 in eval_func /home/fuzz/fuzz/vim/afl/src/eval.c:2113:8
#49 0x6e34ee in eval9 /home/fuzz/fuzz/vim/afl/src/eval.c:4033:9
#50 0x6ef209 in eval8 /home/fuzz/fuzz/vim/afl/src/eval.c:
#51 0x6ecff8 in eval7 /home/fuzz/fuzz/vim/afl/src/eval.
#52 0x6e9f4f in eval6 /home/fuzz/fuzz/vim/afl/src/eval.c:3157:9
```

```
#53 0x6e8aa2 in eval5 /home/fuzz/fuzz/vim/afl/src/eval.c:3046:9
#54 0x6e729c in eval4 /home/fuzz/fuzz/vim/afl/src/eval.c:2897:9
#55 0x6e599f in eval3 /home/fuzz/fuzz/vim/afl/src/eval.c:2758:9

#56 0x6c138f in eval2 /home/fuzz/fuzz/vim/afl/src/eval.c:2632:9
#57 0x6a327f in eval1 /home/fuzz/fuzz/vim/afl/src/eval.c:2478:9
#58 0x6c01d5 in eval0_retarg /home/fuzz/fuzz/vim/afl/src/eval.c:2389:11
#59 0x6a0817 in eval0 /home/fuzz/fuzz/vim/afl/src/eval.c:2364:12
#60 0x6a7475 in eval_to_string_eap /home/fuzz/fuzz/vim/afl/src/eval.c:5
#61 0x6a761f in eval_to_string /home/fuzz/fuzz/vim/afl/src/eval.c:541:1
#62 0xcefa73 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:20
#63 0xcf3b2b in vim_regsub_multi /home/fuzz/fuzz/vim/afl/src/regexp.c:1
#64 0x7b3ed8 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:442
#65 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#66 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#67 0x115d2ac in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#68 0x115939d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#69 0x1153744 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3614
#70 0x1150ae3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#71 0x6e5380 in eval_func /home/fuzz/fuzz/vim/afl/src/eval.c:2113:8
#72 0x6e34ee in eval9 /home/fuzz/fuzz/vim/afl/src/eval.c:4033:9
#73 0x6ef209 in eval8 /home/fuzz/fuzz/vim/afl/src/eval.c:3602:11
#74 0x6ecff8 in eval7 /home/fuzz/fuzz/vim/afl/src/eval.c:3394:9
#75 0x6e9f4f in eval6 /home/fuzz/fuzz/vim/afl/src/eval.c:3157:9
#76 0x6e8aa2 in eval5 /home/fuzz/fuzz/vim/afl/src/eval.c:3046:9
#77 0x6e729c in eval4 /home/fuzz/fuzz/vim/afl/src/eval.c:2897:9
#78 0x6e599f in eval3 /home/fuzz/fuzz/vim/afl/src/eval.c:2758:9
#79 0x6c138f in eval2 /home/fuzz/fuzz/vim/afl/src/eval.c:2632:9
#80 0x6a327f in eval1 /home/fuzz/fuzz/vim/afl/src/eval.c:2478:9
#81 0x6c01d5 in eval0_retarg /home/fuzz/fuzz/vim/afl/src/eval.c:2389:11
#82 0x6a0817 in eval0 /home/fuzz/fuzz/vim/afl/src/eval.c:2364:12
#83 0x6a7475 in eval_to_string_eap /home/fuzz/fuzz/vim/afl/src/eval.c:5
#84 0x6a761f in eval_to_string /home/fuzz/fuzz/vim/afl/src/eval.c:541:1
#85 0xcefa73 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:20
#86 0xcf3b2b in vim_regsub_multi /home/fuzz/fuzz/vim/afl/src/regexp.c:1
#87 0x7b3ed8 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:442
#88 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#89 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#90 0xe5c8fe in do_source_ext /home/fuzz/fuzz/vim/afl/src/
#91 0xe59396 in do_source /home/fuzz/fuzz/vim/afl/src/s
#92 0xe58cd3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:11
```

```
    #93 0xe583de in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1206
    #94 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #95 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1

    #96 0x7cf591 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #97 0x1427482 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #98 0x142361b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #99 0x1418b2d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #100 0x7f8100eab082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31
    #101 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x603000000d95 is located 5 bytes inside of 21-byte region [0x603000000d90,
freed by thread T0 here:
    #0 0x499a52 in free (/home/fuzz/fuzz/vim/afl/src/vim+0x499a52)
    #1 0x4cbdf6 in vim_free /home/fuzz/fuzz/vim/afl/src/alloc.c:625:2
    #2 0xcede83 in regtilde /home/fuzz/fuzz/vim/afl/src/regexp.c:1769:5
    #3 0x7b06d1 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:3997
    #4 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #5 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:17
    #6 0x115d2ac in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:2
    #7 0x115939d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/userfu
    #8 0x1153744 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3614:1
    #9 0x1150ae3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:1834
    #10 0x6e5380 in eval_func /home/fuzz/fuzz/vim/afl/src/eval.c:2113:8
    #11 0x6e34ee in eval9 /home/fuzz/fuzz/vim/afl/src/eval.c:4033:9
    #12 0x6ef209 in eval8 /home/fuzz/fuzz/vim/afl/src/eval.c:3602:11
    #13 0x6ecff8 in eval7 /home/fuzz/fuzz/vim/afl/src/eval.c:3394:9
    #14 0x6e9f4f in eval6 /home/fuzz/fuzz/vim/afl/src/eval.c:3157:9
    #15 0x6e8aa2 in eval5 /home/fuzz/fuzz/vim/afl/src/eval.c:3046:9
    #16 0x6e729c in eval4 /home/fuzz/fuzz/vim/afl/src/eval.c:2897:9
    #17 0x6e599f in eval3 /home/fuzz/fuzz/vim/afl/src/eval.c:2758:9
    #18 0x6c138f in eval2 /home/fuzz/fuzz/vim/afl/src/eval.c:2632:9
    #19 0x6a327f in eval1 /home/fuzz/fuzz/vim/afl/src/eval.c:2478:9
    #20 0x6c01d5 in eval0_retarg /home/fuzz/fuzz/vim/afl/src/eval.c:2389:11
    #21 0x6a0817 in eval0 /home/fuzz/fuzz/vim/afl/src/eval.c:2364:12
    #22 0x6a7475 in eval_to_string_eap /home/fuzz/fuzz/vim/afl/src/eval.c:5
    #23 0x6a761f in eval_to_string /home/fuzz/fuzz/vim/afl/src/eval.c:541:1
    #24 0xcefa73 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:26
    #25 0xcf3b2b in vim_regsub_multi /home/fuzz/fuzz/vim/afl/
    #26 0x7b3ed8 in ex_substitute /home/fuzz/fuzz/vim/afl/s
    #27 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
```

```
    #28 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #29 0x115d2ac in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:


previously allocated by thread T0 here:
    #0 0x499cbd in malloc (/home/fuzz/fuzz/vim/afl/src/vim+0x499cbd)
    #1 0x4cb392 in lalloc /home/fuzz/fuzz/vim/afl/src/alloc.c:246:11
    #2 0x4cb27a in alloc /home/fuzz/fuzz/vim/afl/src/alloc.c:151:12
    #3 0xced8fc in regtilde /home/fuzz/fuzz/vim/afl/src/regexp.c:1735:12
    #4 0x7b06d1 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:3997
    #5 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #6 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:17
    #7 0x115d2ac in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:2
    #8 0x115939d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/userfu
    #9 0x1153744 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3614:1
    #10 0x1150ae3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
    #11 0x6e5380 in eval_func /home/fuzz/fuzz/vim/afl/src/eval.c:2113:8
    #12 0x6e34ee in eval9 /home/fuzz/fuzz/vim/afl/src/eval.c:4033:9
    #13 0x6ef209 in eval8 /home/fuzz/fuzz/vim/afl/src/eval.c:3602:11
    #14 0x6ecff8 in eval7 /home/fuzz/fuzz/vim/afl/src/eval.c:3394:9
    #15 0x6e9f4f in eval6 /home/fuzz/fuzz/vim/afl/src/eval.c:3157:9
    #16 0x6e8aa2 in eval5 /home/fuzz/fuzz/vim/afl/src/eval.c:3046:9
    #17 0x6e729c in eval4 /home/fuzz/fuzz/vim/afl/src/eval.c:2897:9
    #18 0x6e599f in eval3 /home/fuzz/fuzz/vim/afl/src/eval.c:2758:9
    #19 0x6c138f in eval2 /home/fuzz/fuzz/vim/afl/src/eval.c:2632:9
    #20 0x6a327f in eval1 /home/fuzz/fuzz/vim/afl/src/eval.c:2478:9
    #21 0x6c01d5 in eval0_retarg /home/fuzz/fuzz/vim/afl/src/eval.c:2389:11
    #22 0x6a0817 in eval0 /home/fuzz/fuzz/vim/afl/src/eval.c:2364:12
    #23 0x6a7475 in eval_to_string_eap /home/fuzz/fuzz/vim/afl/src/eval.c:5
    #24 0x6a761f in eval_to_string /home/fuzz/fuzz/vim/afl/src/eval.c:541:1
    #25 0xcefa73 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:26
    #26 0xcf3b2b in vim_regsub_multi /home/fuzz/fuzz/vim/afl/src/regexp.c:1
    #27 0x7b3ed8 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:442
    #28 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #29 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/vim/afl/src/
Shadow bytes around the buggy address:
  0x0c067fff8160: 07 fa fa fa 00 00 06 fa fa fa 00 00 07 fa f
  0x0c067fff8170: 00 00 00 fa fa fa 00 00 06 fa fa fa 00 00
  0x0c067fff8180: fa fa 00 00 00 02 fa fa 00 00 00 01 fa fa 00 00
```

```
  0x0c067fff8190: 07 fa fa fa 00 00 04 fa fa fa 00 00 00 01 fa fa
  0x0c067fff81a0: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 05 fa
=>0x0c067fff81b0: fa fa[fd]fd fd fa fa fa 00 00 03 fa fa fa 00 00

  0x0c067fff81c0: 00 02 fa fa 00 00 00 fa fa fa fd fd fd fd fa fa
  0x0c067fff81d0: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x0c067fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8200: 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
==10794==ABORTING
```

poc_huaf4_s.dat

Impact

This vulnerability is capable of crashing software, modify memory, and possible remote execution.

CVE

CVE-2022-2345
(Published)

Vulnerability Type

CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 771 times.

We are processing your report and will contact the **vim** team within 24 hours. 5 months ago

We have contacted a member of the **vim** team and are waiting to hear back 5 months ago

Bram Moolenaar validated this vulnerability 5 months ago

Can reproduc it, POC is nicely short.

Chat with us

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 marked this as fixed in 9.0.0046 with commit 32acf1 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation