Use After Free in function find_var_also_in_script in vim/vim

0

Valid Reported on Aug 16th 2022

Description

Use After Free in function find_var_also_in_script at vim/src/evalvars.c:3174

vim version

```
git log
commit 887748742deae3d6de7aa0fdbb042afe1ccf5e7a (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S /home/fuzz/test/poc3_huaf.dat -c :qa!
==================================================================
==101656==ERROR: AddressSanitizer: heap-use-after-free on address 0x611000(
READ of size 1 at 0x611000000cc2 thread T0
    #0 0x7f97f6872926 in __interceptor_strncmp ../../../../src/libsanitizer
    #1 0x563585be6150 in find_var_also_in_script /home/fuzz/vim/src/evalvar
    #2 0x563585b87e5d in deref_function_name /home/fuzz/vim/src/eval.c:647
    #3 0x563585b9d753 in eval_method /home/fuzz/vim/src/eval.c:4358
    #4 0x563585ba73c0 in handle_subscript /home/fuzz/vim/src/eval.c:6417
    #5 0x563585b9bf31 in eval9 /home/fuzz/vim/src/eval.c:4063
    #6 0x563585b99ecc in eval8 /home/fuzz/vim/src/eval.c:3602
    #7 0x563585b98e67 in eval7 /home/fuzz/vim/src/eval.c:3394
    #8 0x563585b97867 in eval6 /home/fuzz/vim/src/eval.c:3157
    #9 0x563585b96e58 in eval5 /home/fuzz/vim/src/eval.c:304
    #10 0x563585b96027 in eval4 /home/fuzz/vim/src/eval.c:2
    #11 0x563585b9542e in eval3 /home/fuzz/vim/src/eval.c:2758
```

```
    #12 0x563585b9489f in eval2 /home/fuzz/vim/src/eval.c:2632
    #13 0x563585b93724 in eval1 /home/fuzz/vim/src/eval.c:2478
    #14 0x563585b9cfbe in eval_lambda /home/fuzz/vim/src/eval.c:4267

    #15 0x563585ba7395 in handle_subscript /home/fuzz/vim/src/eval.c:6414
    #16 0x563585b9bf31 in eval9 /home/fuzz/vim/src/eval.c:4063
    #17 0x563585b99ecc in eval8 /home/fuzz/vim/src/eval.c:3602
    #18 0x563585b98e67 in eval7 /home/fuzz/vim/src/eval.c:3394
    #19 0x563585b97867 in eval6 /home/fuzz/vim/src/eval.c:3157
    #20 0x563585b96e58 in eval5 /home/fuzz/vim/src/eval.c:3046
    #21 0x563585b96027 in eval4 /home/fuzz/vim/src/eval.c:2897
    #22 0x563585b9542e in eval3 /home/fuzz/vim/src/eval.c:2758
    #23 0x563585b9489f in eval2 /home/fuzz/vim/src/eval.c:2632
    #24 0x563585b93724 in eval1 /home/fuzz/vim/src/eval.c:2478
    #25 0x563585b92fa0 in eval0_retarg /home/fuzz/vim/src/eval.c:2389
    #26 0x563585b92da2 in eval0 /home/fuzz/vim/src/eval.c:2364
    #27 0x563585c4b021 in ex_eval /home/fuzz/vim/src/ex_eval.c:951
    #28 0x563585c1e453 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #29 0x563585c156f6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #30 0x563585f3887b in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #31 0x563585f399ad in do_source /home/fuzz/vim/src/scriptfile.c:1803
    #32 0x563585f36515 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #33 0x563585f3657a in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #34 0x563585c1e453 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #35 0x563585c156f6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #36 0x563585c13a90 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #37 0x563586210005 in exe_commands /home/fuzz/vim/src/main.c:3133
    #38 0x563586209173 in vim_main2 /home/fuzz/vim/src/main.c:780
    #39 0x563586208a2b in main /home/fuzz/vim/src/main.c:432
    #40 0x7f97f6411082 in __libc_start_main ../csu/libc-start.c:308
    #41 0x563585a94e4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x611000000cc2 is located 2 bytes inside of 250-byte region [0x611000000cc0
freed by thread T0 here:
    #0 0x7f97f68a840f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x563585a9553a in vim_free /home/fuzz/vim/src/alloc.c:625
    #2 0x563585b928b0 in eval_next_line /home/fuzz/vim/src/eval.c:2277
    #3 0x563585ba66bb in handle_subscript /home/fuzz/vim/src/eval.c:6317
    #4 0x563585b9bf31 in eval9 /home/fuzz/vim/src/eval.c:406
    #5 0x563585b87e40 in deref_function_name /home/fuzz/vim
    #6 0x563585b9d753 in eval_method /home/fuzz/vim/src/eval.c:4358
```

```
    #7 0x563585ba73c0 in handle_subscript /home/fuzz/vim/src/eval.c:6417
    #8 0x563585b9bf31 in eval9 /home/fuzz/vim/src/eval.c:4063
    #9 0x563585b99ecc in eval8 /home/fuzz/vim/src/eval.c:3602

    #10 0x563585b98e67 in eval7 /home/fuzz/vim/src/eval.c:3394
    #11 0x563585b97867 in eval6 /home/fuzz/vim/src/eval.c:3157
    #12 0x563585b96e58 in eval5 /home/fuzz/vim/src/eval.c:3046
    #13 0x563585b96027 in eval4 /home/fuzz/vim/src/eval.c:2897
    #14 0x563585b9542e in eval3 /home/fuzz/vim/src/eval.c:2758
    #15 0x563585b9489f in eval2 /home/fuzz/vim/src/eval.c:2632
    #16 0x563585b93724 in eval1 /home/fuzz/vim/src/eval.c:2478
    #17 0x563585b9cfbe in eval_lambda /home/fuzz/vim/src/eval.c:4267
    #18 0x563585ba7395 in handle_subscript /home/fuzz/vim/src/eval.c:6414
    #19 0x563585b9bf31 in eval9 /home/fuzz/vim/src/eval.c:4063
    #20 0x563585b99ecc in eval8 /home/fuzz/vim/src/eval.c:3602
    #21 0x563585b98e67 in eval7 /home/fuzz/vim/src/eval.c:3394
    #22 0x563585b97867 in eval6 /home/fuzz/vim/src/eval.c:3157
    #23 0x563585b96e58 in eval5 /home/fuzz/vim/src/eval.c:3046
    #24 0x563585b96027 in eval4 /home/fuzz/vim/src/eval.c:2897
    #25 0x563585b9542e in eval3 /home/fuzz/vim/src/eval.c:2758
    #26 0x563585b9489f in eval2 /home/fuzz/vim/src/eval.c:2632
    #27 0x563585b93724 in eval1 /home/fuzz/vim/src/eval.c:2478
    #28 0x563585b92fa0 in eval0_retarg /home/fuzz/vim/src/eval.c:2389
    #29 0x563585b92da2 in eval0 /home/fuzz/vim/src/eval.c:2364

previously allocated by thread T0 here:
    #0 0x7f97f68a8c3e in __interceptor_realloc ../../../../src/libsanitizer
    #1 0x563585a95cf0 in ga_grow_inner /home/fuzz/vim/src/alloc.c:757
    #2 0x563585a95aed in ga_grow /home/fuzz/vim/src/alloc.c:722
    #3 0x563585f3a2e7 in get_one_sourceline /home/fuzz/vim/src/scriptfile.c
    #4 0x563585f3b197 in getsourceline /home/fuzz/vim/src/scriptfile.c:2128
    #5 0x563585c14e84 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:875
    #6 0x563585f3887b in do_source_ext /home/fuzz/vim/src/scriptfile.c:1674
    #7 0x563585f399ad in do_source /home/fuzz/vim/src/scriptfile.c:1803
    #8 0x563585f36515 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #9 0x563585f3657a in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #10 0x563585c1e453 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #11 0x563585c156f6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #12 0x563585c13a90 in do_cmdline_cmd /home/fuzz/vim/src/
    #13 0x563586210005 in exe_commands /home/fuzz/vim/src/m
    #14 0x563586209173 in vim_main2 /home/fuzz/vim/src/main.c:780
```

```
    #15 0x563586208a2b in main /home/fuzz/vim/src/main.c:432
    #16 0x7f97f6411082 in __libc_start_main ../csu/libc-start.c:308


SUMMARY: AddressSanitizer: heap-use-after-free ../../../../src/libsanitizer
Shadow bytes around the buggy address:
  0x0c227fff8140: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c227fff8150: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c227fff8160: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x0c227fff8170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c227fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02
=>0x0c227fff8190: fa fa fa fa fa fa fa fa[fd]fd fd fd fd fd fd fd
  0x0c227fff81a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c227fff81b0: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x0c227fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c227fff81d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02
  0x0c227fff81e0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
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
==101656==ABORTING
```

poc3_huaf.dat

Impact

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

CVE
CVE-2022-2889
(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

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. The POC can be shortened, a few lines can be removed without changing the reproduction.

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 9.0.0225

Bram Moolenaar marked this as fixed in **9.0.0224** with commit **91c7cb** 3 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation

home
hacktivity
leaderboard
FAQ
contact us
terms
privacy policy

company
about
team