Use After Free in function movemark in vim/vim

1

Valid Reported on Sep 19th 2022

Description

Use After Free in function movemark at mark.c:234.

vim version

```
git log
commit bcd6924245c0e73d8be256282656c06aaf91f17c (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/fuzz/test/poc10_huaf.dat -
==================================================================
==6729==ERROR: AddressSanitizer: heap-use-after-free on address 0x62500000d
READ of size 16 at 0x62500000d910 thread T0
    #0 0x559ab291177e in movemark /home/fuzz/vim/src/mark.c:234
    #1 0x559ab29b712e in nv_pcmark /home/fuzz/vim/src/normal.c:5378
    #2 0x559ab29a7c75 in nv_ctrlo /home/fuzz/vim/src/normal.c:3309
    #3 0x559ab299a51b in normal_cmd /home/fuzz/vim/src/normal.c:937
    #4 0x559ab281b8e5 in exec_normal /home/fuzz/vim/src/ex_docmd.c:8844
    #5 0x559ab281b6a4 in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:8807
    #6 0x559ab281af48 in ex_normal /home/fuzz/vim/src/ex_docmd.c:8725
    #7 0x559ab27f73ea in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #8 0x559ab27ee646 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #9 0x559ab2b13fbd in do_source_ext /home/fuzz/vim/src/scriptfile.c:1667
    #10 0x559ab2b151f2 in do_source /home/fuzz/vim/src/scriptfile.c:1811
    #11 0x559ab2b11cb0 in cmd_source /home/fuzz/vim/src/scr
    #12 0x559ab2b11d15 in ex_source /home/fuzz/vim/src/script
    #13 0x559ab27f73ea in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
```

```
    #14 0x559ab27ee646 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #15 0x559ab27ec9e0 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #16 0x559ab2df67cb in exe_commands /home/fuzz/vim/src/main.c:3139
    #17 0x559ab2def934 in vim_main2 /home/fuzz/vim/src/main.c:781
    #18 0x559ab2def1ec in main /home/fuzz/vim/src/main.c:432
    #19 0x7fb4b8f89082 in __libc_start_main ../csu/libc-start.c:308
    #20 0x559ab266be4d in _start (/home/fuzz/vim/src/vim+0x13be4d)

0x62500000d910 is located 4112 bytes inside of 9120-byte region [0x62500000
freed by thread T0 here:
    #0 0x7fb4b942040f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x559ab266c576 in vim_free /home/fuzz/vim/src/alloc.c:623
    #2 0x559ab2681257 in apply_autocmds_group /home/fuzz/vim/src/autocmd.c:
    #3 0x559ab267f4b2 in apply_autocmds_retval /home/fuzz/vim/src/autocmd.c
    #4 0x559ab27dabe8 in do_ecmd /home/fuzz/vim/src/ex_cmds.c:3038
    #5 0x559ab27d81b1 in getfile /home/fuzz/vim/src/ex_cmds.c:2411
    #6 0x559ab2693873 in buflist_getfile /home/fuzz/vim/src/buffer.c:2445
    #7 0x559ab2911701 in movemark /home/fuzz/vim/src/mark.c:230
    #8 0x559ab29b712e in nv_pcmark /home/fuzz/vim/src/normal.c:5378
    #9 0x559ab29a7c75 in nv_ctrlo /home/fuzz/vim/src/normal.c:3309
    #10 0x559ab299a51b in normal_cmd /home/fuzz/vim/src/normal.c:937
    #11 0x559ab281b8e5 in exec_normal /home/fuzz/vim/src/ex_docmd.c:8844
    #12 0x559ab281b6a4 in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:886
    #13 0x559ab281af48 in ex_normal /home/fuzz/vim/src/ex_docmd.c:8725
    #14 0x559ab27f73ea in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #15 0x559ab27ee646 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #16 0x559ab2b13fbd in do_source_ext /home/fuzz/vim/src/scriptfile.c:166
    #17 0x559ab2b151f2 in do_source /home/fuzz/vim/src/scriptfile.c:1811
    #18 0x559ab2b11cb0 in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #19 0x559ab2b11d15 in ex_source /home/fuzz/vim/src/scriptfile.c:1189
    #20 0x559ab27f73ea in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #21 0x559ab27ee646 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #22 0x559ab27ec9e0 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #23 0x559ab2df67cb in exe_commands /home/fuzz/vim/src/main.c:3139
    #24 0x559ab2def934 in vim_main2 /home/fuzz/vim/src/main.c:781
    #25 0x559ab2def1ec in main /home/fuzz/vim/src/main.c:432
    #26 0x7fb4b8f89082 in __libc_start_main ../csu/libc-start.c:308

previously allocated by thread T0 here:
    #0 0x7fb4b9420808 in __interceptor_malloc ../../../../src/libsanitizer/
```

```
    #1 0x559ab266c28a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x559ab266c120 in alloc_clear /home/fuzz/vim/src/alloc.c:177
    #3 0x559ab2d554e4 in win_alloc /home/fuzz/vim/src/window.c:5080

    #4 0x559ab2d40ff9 in win_split_ins /home/fuzz/vim/src/window.c:1107
    #5 0x559ab2d3f8b9 in win_split /home/fuzz/vim/src/window.c:846
    #6 0x559ab26726ac in do_argfile /home/fuzz/vim/src/arglist.c:708
    #7 0x559ab26723f9 in ex_argument /home/fuzz/vim/src/arglist.c:674
    #8 0x559ab27f73ea in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #9 0x559ab27ee646 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #10 0x559ab2b13fbd in do_source_ext /home/fuzz/vim/src/scriptfile.c:166
    #11 0x559ab2b151f2 in do_source /home/fuzz/vim/src/scriptfile.c:1811
    #12 0x559ab2b11cb0 in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #13 0x559ab2b11d15 in ex_source /home/fuzz/vim/src/scriptfile.c:1189
    #14 0x559ab27f73ea in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #15 0x559ab27ee646 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #16 0x559ab27ec9e0 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #17 0x559ab2df67cb in exe_commands /home/fuzz/vim/src/main.c:3139
    #18 0x559ab2def934 in vim_main2 /home/fuzz/vim/src/main.c:781
    #19 0x559ab2def1ec in main /home/fuzz/vim/src/main.c:432
    #20 0x7fb4b8f89082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/vim/src/mark.c:23
Shadow bytes around the buggy address:
  0x0c4a7fff9ad0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9ae0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9af0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b00: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b10: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c4a7fff9b20: fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff9b70: 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
  ==6729==ABORTING
```

poc download url: https://github.com/Janette88/vim/blob/main/poc10_huaf.dat

Impact

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

Occurrences

C mark.c L234

CVE
CVE-2022-3256
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,172 times.

We are processing your report and will contact the **vim** team within 24 hours. 2 months ago

We have contacted a member of the **vim** team and are waiting to hear back 2 months ago

Bram Moolenaar validated this vulnerability 2 months ago

I can reproduce it. The POC can be further simplified and then used in a regression test.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 2 months ago

Fixed with patch 9.0.0530

Bram Moolenaar marked this as fixed in 9.0.0530 with commit 8ecfa2 2 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

mark.c#L234 has been validated ✔

Sign in to join this conversation