Use After Free in function getcmdline_int in vim/vim

0

Valid Reported on Sep 14th 2022

Description

Use After Free in function getcmdline_int at vim/src/ex_getln.c:2547.

vim version

```
git log
commit 470a14140bc06f1653edf26ab0b3c9b801080353 (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/fuzz/test/poc9_huaf.dat -c
==================================================================
==131703==ERROR: AddressSanitizer: heap-use-after-free on address 0x625000(
READ of size 8 at 0x625000006398 thread T0
    #0 0x558844bd1585 in getcmdline_int /home/fuzz/vim/src/ex_getln.c:2547
    #1 0x558844bcc84e in getcmdline /home/fuzz/vim/src/ex_getln.c:1554
    #2 0x558844d4420d in nv_search /home/fuzz/vim/src/normal.c:4158
    #3 0x558844d30c1e in normal_cmd /home/fuzz/vim/src/normal.c:937
    #4 0x558844bb218b in exec_normal /home/fuzz/vim/src/ex_docmd.c:8825
    #5 0x558844bb1f4a in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:878(
    #6 0x558844bb17ee in ex_normal /home/fuzz/vim/src/ex_docmd.c:8706
    #7 0x558844b8df7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #8 0x558844b851d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #9 0x558844eaa77c in do_source_ext /home/fuzz/vim/src/scriptfile.c:1664
    #10 0x558844eab9b1 in do_source /home/fuzz/vim/src/scriptfile.c:1808
    #11 0x558844ea846f in cmd_source /home/fuzz/vim/src/scr
    #12 0x558844ea84d4 in ex_source /home/fuzz/vim/src/script
    #13 0x558844b8df7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
```

Chat with us

```
    #14 0x558844b851d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #15 0x558844b83572 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #16 0x5588451888be in exe_commands /home/fuzz/vim/src/main.c:3139
    #17 0x558845181a27 in vim_main2 /home/fuzz/vim/src/main.c:781
    #18 0x5588451812df in main /home/fuzz/vim/src/main.c:432
    #19 0x7f105ec28082 in __libc_start_main ../csu/libc-start.c:308
    #20 0x558844a02e4d in _start (/home/fuzz/vim/src/vim+0x13ae4d)

0x625000006398 is located 4760 bytes inside of 9360-byte region [0x62500000
freed by thread T0 here:
    #0 0x7f105f0bf40f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x558844a03576 in vim_free /home/fuzz/vim/src/alloc.c:623
    #2 0x558844a18186 in apply_autocmds_group /home/fuzz/vim/src/autocmd.c:
    #3 0x558844a163bf in apply_autocmds /home/fuzz/vim/src/autocmd.c:1702
    #4 0x5588450e6f3e in win_enter_ext /home/fuzz/vim/src/window.c:4977
    #5 0x5588450e63ba in win_enter /home/fuzz/vim/src/window.c:4838
    #6 0x5588450e5693 in win_goto /home/fuzz/vim/src/window.c:4614
    #7 0x558844bda6fe in open_cmdwin /home/fuzz/vim/src/ex_getln.c:4646
    #8 0x558844bce99f in getcmdline_int /home/fuzz/vim/src/ex_getln.c:1932
    #9 0x558844bcc84e in getcmdline /home/fuzz/vim/src/ex_getln.c:1554
    #10 0x558844d4420d in nv_search /home/fuzz/vim/src/normal.c:4158
    #11 0x558844d30c1e in normal_cmd /home/fuzz/vim/src/normal.c:937
    #12 0x558844bb218b in exec_normal /home/fuzz/vim/src/ex_docmd.c:8825
    #13 0x558844bb1f4a in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:878
    #14 0x558844bb17ee in ex_normal /home/fuzz/vim/src/ex_docmd.c:8706
    #15 0x558844b8df7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #16 0x558844b851d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #17 0x558844eaa77c in do_source_ext /home/fuzz/vim/src/scriptfile.c:166
    #18 0x558844eab9b1 in do_source /home/fuzz/vim/src/scriptfile.c:1808
    #19 0x558844ea846f in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #20 0x558844ea84d4 in ex_source /home/fuzz/vim/src/scriptfile.c:1189
    #21 0x558844b8df7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #22 0x558844b851d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #23 0x558844b83572 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #24 0x5588451888be in exe_commands /home/fuzz/vim/src/main.c:3139
    #25 0x558845181a27 in vim_main2 /home/fuzz/vim/src/main.c:781
    #26 0x5588451812df in main /home/fuzz/vim/src/main.c:432
    #27 0x7f105ec28082 in __libc_start_main ../csu/libc-start

previously allocated by thread T0 here:
```

Chat with us

```
    #0 0x7f105f0bf808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x558844a0328a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x558844a03120 in alloc_clear /home/fuzz/vim/src/alloc.c:177

    #3 0x558844a28923 in buflist_new /home/fuzz/vim/src/buffer.c:2081
    #4 0x5588450e21af in win_alloc_firstwin /home/fuzz/vim/src/window.c:387
    #5 0x5588450e1d06 in win_alloc_first /home/fuzz/vim/src/window.c:3804
    #6 0x558845181d71 in common_init /home/fuzz/vim/src/main.c:975
    #7 0x558845180fed in main /home/fuzz/vim/src/main.c:185
    #8 0x7f105ec28082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/vim/src/ex_getln.
Shadow bytes around the buggy address:
  0x0c4a7fff8c20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8c30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8c40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8c50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8c60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c4a7fff8c70: fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8c80: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8c90: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8ca0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8cb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c4a7fff8cc0: 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
```

Chat with us

```
    Left alloca redzone:     ca
    Right alloca redzone:    cb
    Shadow gap:              cc

  ==131703==ABORTING
```

poc download url:
https://github.com/Janette88/vim/blob/main/poc9_huaf.dat

Impact

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

Occurrences

C ex_getln.c L2547

CVE
CVE-2022-3235
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
janette88

Chat with us

@janette88

master

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,171 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. With some effort I can use the POC for 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 Maintainer

Fixed with patch 9.0.0490

Bram Moolenaar marked this as fixed in **9.0.0490** with commit **1c3dd8** 2 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

ex_getln.c#L2547 has been validated ✓

Chat with us

Sign in to join this conversation

2022 © 418sec

Chat with us