# Use after free in append_command in vim/vim

0

✓ Valid Reported on Apr 28th 2022

## ✍️ Description

When fuzzing vim commit `fc78a0369` (works with latest build and latest commit `202b4bd3a` per this time of this report) with clang 13 and ASan, I discovered a buffer overflow.

## Proof of Concept

Here is the poc

```
https://drive.google.com/file/d/1QFs9OysjzlRQP4hmfnMdfohaEg8lIZ8y/view?usp=
```

How to build

```
LD=lld AS=llvm-as AR=llvm-ar RANLIB=llvm-ranlib CC=clang CXX=clang++ CFLAGS
make -j$(nproc)
```

Proof of Concept
Run crafted file with this command
`./vim -u NONE -X -Z -e -s -S poc_mb_copy_char_min -c :qa!`
ASan stack trace:

```
aldo@vps:~/vimbaru/src$ ASAN_OPTIONS=symbolize=1 ASAN_SYMBOLIZER_PATH=/usr/
=================================================================
==829948==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000
WRITE of size 1 at 0x619000000e81 thread T0
    #0 0x6fc615 in append_command /home/aldo/vimtes/src/ex_
    #1 0x6d705d in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2018:6
    #2 0x6ca342 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #2 0x6ca342 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #3 0xafd4a5 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1674:5
    #4 0xafaef0 in do_source /home/aldo/vimtes/src/scriptfile.c:1801:12
    #5 0xafaa29 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1174:14
    #6 0xafa50d in ex_source /home/aldo/vimtes/src/scriptfile.c:1200:2
    #7 0x6d6612 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #8 0x6ca342 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #9 0x6cd5d0 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:586:12
    #10 0xed6bb4 in exe_commands /home/aldo/vimtes/src/main.c:3108:2
    #11 0xed48e9 in vim_main2 /home/aldo/vimtes/src/main.c:780:2
    #12 0xece1d0 in main /home/aldo/vimtes/src/main.c:432:12
    #13 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #14 0x41edcd in _start (/home/aldo/vimtes/src/vim+0x41edcd)

0x619000000e81 is located 0 bytes to the right of 1025-byte region [0x61900
allocated by thread T0 here:
    #0 0x499c8d in malloc (/home/aldo/vimtes/src/vim+0x499c8d)
    #1 0x4cb0e0 in lalloc /home/aldo/vimtes/src/alloc.c:246:11
    #2 0x4cb039 in alloc /home/aldo/vimtes/src/alloc.c:151:12
    #3 0xece209 in common_init /home/aldo/vimtes/src/main.c:914:19
    #4 0xecdd84 in main /home/aldo/vimtes/src/main.c:185:5
    #5 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/c

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/aldo/vimtes/src/ex_dc
Shadow bytes around the buggy address:
  0x0c327fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff81d0:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 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
==829948==ABORTING
```

## Impact

This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution

CVE
CVE-2022-1616
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.3)

Registry
Other

Affected Version
8.2.4843

Visibility
Public

Status

Fixed

Found by

Muhammad Aldo Firmansyah

@thecrott

legend

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,307 times.

We are processing your report and will contact the **vim** team within 24 hours. 7 months ago

Muhammad Aldo Firmansyah modified the report 7 months ago

We have contacted a member of the **vim** team and are waiting to hear back 7 months ago

We have sent a follow up to the **vim** team. We will try again in 7 days. 7 months ago

Bram Moolenaar validated this vulnerability 7 months ago

Can reproduce, caused by multiple composing characters.

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 7 months ago Maintainer

Fixed in patch 8.2.4895.

Bram Moolenaar marked this as fixed in 8.2 with commit d88934 7 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

xiaoge1001 6 months ago

@thecrott I'm very sorry. It's not convenient for me to visit the POC file download address and can't download it. Can you provide the contents of the POC file here or upload the POC file to GitHub? Thank you very much.
I use vim-8.2. I analyze the code and think it is affected, but I need to reproduce the problem.

Bram Moolenaar 6 months ago Maintainer

Patch 8.2.4895 adds Test_report_error_with_composing() which should reproduce the problem without the fix.

Sign in to join this conversation

terms

privacy policy

Chat with us