Use After Free in function utf_ptr2char in vim/vim

0

Valid Reported on May 30th 2022

Description

Use After Free in function utf_ptr2char at mbyte.c:1794

vim version

```
git log
commit be99042b03edf7b8156c9adbc23516bfcf2cec0f (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_huaf2_s.dat -c :qa!
==================================================================
==8341==ERROR: AddressSanitizer: heap-use-after-free on address 0x602000007
READ of size 1 at 0x6020000070f1 thread T0
    #0 0xa46fe8 in utf_ptr2char /home/fuzz/fuzz/vim/vim/src/mbyte.c:1794:9
    #1 0xd9b882 in nfa_regmatch /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.c:
    #2 0xd98745 in nfa_regtry /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.c:72
    #3 0xd96437 in nfa_regexec_both /home/fuzz/fuzz/vim/vim/src/./regexp_nf
    #4 0xcf85c8 in nfa_regexec_nl /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.
    #5 0xcf4835 in vim_regexec_string /home/fuzz/fuzz/vim/vim/src/regexp.c:
    #6 0xcf5079 in vim_regexec /home/fuzz/fuzz/vim/vim/src/regexp.c:2816:12
    #7 0xe8ce76 in find_pattern_in_path /home/fuzz/fuzz/vim/vim/src/search.
    #8 0x81ea0f in ex_findpat /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8869:2
    #9 0x7dd539 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:2
    #10 0x7ca2a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/
    #11 0xe59ecc in do_source_ext /home/fuzz/fuzz/vim/vim/src/
    #12 0xe56926 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
```

```
    #13 0xe5625c in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #14 0xe5593e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #15 0x7dd539 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #16 0x7ca2a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #17 0x7cef41 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #18 0x1425eb2 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #19 0x142204b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #20 0x1417745 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #21 0x7fe8c60f1082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #22 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x6020000070f1 is located 1 bytes inside of 2-byte region [0x6020000070f0,0
freed by thread T0 here:
    #0 0x499a62 in free (/home/fuzz/fuzz/vim/vim/src/vim+0x499a62)
    #1 0x4cbe06 in vim_free /home/fuzz/fuzz/vim/vim/src/alloc.c:621:2
    #2 0xa65e45 in ml_flush_line /home/fuzz/fuzz/vim/vim/src/memline.c:4063
    #3 0xa7b645 in ml_get_buf /home/fuzz/fuzz/vim/vim/src/memline.c:2651:2
    #4 0xa7bdf6 in ml_get_pos /home/fuzz/fuzz/vim/vim/src/memline.c:2573:13
    #5 0xaad44d in gchar_pos /home/fuzz/fuzz/vim/vim/src/misc1.c:521:11
    #6 0x10ab5e0 in findsent /home/fuzz/fuzz/vim/vim/src/textobject.c:101:1
    #7 0xa1c3be in getmark_buf_fnum /home/fuzz/fuzz/vim/vim/src/mark.c:354:
    #8 0xa1b989 in getmark_buf /home/fuzz/fuzz/vim/vim/src/mark.c:287:12
    #9 0xda7f3a in nfa_regmatch /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.c:
    #10 0xd98745 in nfa_regtry /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.c:7
    #11 0xd96437 in nfa_regexec_both /home/fuzz/fuzz/vim/vim/src/./regexp_n
    #12 0xcf85c8 in nfa_regexec_nl /home/fuzz/fuzz/vim/vim/src/./regexp_nfa
    #13 0xcf4835 in vim_regexec_string /home/fuzz/fuzz/vim/vim/src/regexp.c
    #14 0xcf5079 in vim_regexec /home/fuzz/fuzz/vim/vim/src/regexp.c:2816:1
    #15 0xe8ce76 in find_pattern_in_path /home/fuzz/fuzz/vim/vim/src/search
    #16 0x81ea0f in ex_findpat /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8869:
    #17 0x7dd539 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #18 0x7ca2a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #19 0xe59ecc in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #20 0xe56926 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #21 0xe5625c in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #22 0xe5593e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #23 0x7dd539 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #24 0x7ca2a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #25 0x7cef41 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/
    #26 0x1425eb2 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
```

```
    #27 0x142204b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #28 0x1417745 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #29 0x7fe8c60f1082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/


previously allocated by thread T0 here:
    #0 0x499ccd in malloc (/home/fuzz/fuzz/vim/vim/src/vim+0x499ccd)
    #1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x54d5ed in ins_char_bytes /home/fuzz/fuzz/vim/vim/src/change.c:1095
    #4 0x54e2cb in ins_char /home/fuzz/fuzz/vim/vim/src/change.c:1010:5
    #5 0x69714f in insertchar /home/fuzz/fuzz/vim/vim/src/edit.c:2276:6
    #6 0x68f1e9 in insert_special /home/fuzz/fuzz/vim/vim/src/edit.c:2039:2
    #7 0x6749d2 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1360:3
    #8 0xb98bd7 in op_change /home/fuzz/fuzz/vim/vim/src/ops.c:1752:14
    #9 0xbb2867 in do_pending_operator /home/fuzz/fuzz/vim/vim/src/ops.c:40
    #10 0xb21fc3 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:963:2
    #11 0x8153ae in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8792
    #12 0x814bd8 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:
    #13 0x814789 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8673:6
    #14 0x7dd539 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #15 0x7ca2a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #16 0xe59ecc in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #17 0xe56926 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #18 0xe5625c in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #19 0xe5593e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #20 0x7dd539 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #21 0x7ca2a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #22 0x7cef41 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #23 0x1425eb2 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #24 0x142204b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #25 0x1417745 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #26 0x7fe8c60f1082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/vim/vim/src/
Shadow bytes around the buggy address:
  0x0c047fff8dc0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fa
  0x0c047fff8dd0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8de0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8df0: fa fa fd fa fa fa fd fa fa fa 02 fa fa fa
  0x0c047fff8e00: fa fa 00 fa fa fa 01 fa fa fa 01 fa fa fa 00 00
```

```
=>0x0c047fff8e10: fa fa 01 fa fa fa 02 fa fa fa fd fa fa fa[fd]fa
  0x0c047fff8e20: fa fa 05 fa fa fa fd fd fa fa 00 01 fa fa 00 00
  0x0c047fff8e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

  0x0c047fff8e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e60: 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
==8341==ABORTING
```

poc_huaf2_s.dat

Impact

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

CVE
CVE-2022-1968
(Published)

(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,545 times.

We are processing your report and will contact the **vim** team within 24 hours. 6 months ago

We have contacted a member of the **vim** team and are waiting to hear back 6 months ago

Bram Moolenaar validated this vulnerability 6 months ago

I can reproduce, another case where a pointer is kept that becomes invalid.

TDHX ICS Security has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar marked this as fixed in **8.2** with commit **409510** 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation