Heap-based Buffer Overflow in function utfc_ptr2len in vim/vim

0

Valid Reported on Sep 13th 2022

Description

Heap-based Buffer Overflow in function utfc_ptr2len at vim/src/mbyte.c:2125.

vim version

```
git log
commit 470a14140bc06f1653edf26ab0b3c9b801080353 (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/fuzz/test/poc6_hbo.dat -c
==================================================================
==130015==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000
READ of size 1 at 0x6020000063f2 thread T0
    #0 0x557b66342c94 in utfc_ptr2len /home/fuzz/vim/src/mbyte.c:2125
    #1 0x557b6637ddca in inc /home/fuzz/vim/src/misc2.c:360
    #2 0x557b6637dca4 in inc_cursor /home/fuzz/vim/src/misc2.c:337
    #3 0x557b663e6139 in op_replace /home/fuzz/vim/src/ops.c:1235
    #4 0x557b663fdce4 in do_pending_operator /home/fuzz/vim/src/ops.c:4200
    #5 0x557b663b3dce in normal_cmd /home/fuzz/vim/src/normal.c:959
    #6 0x557b6623518b in exec_normal /home/fuzz/vim/src/ex_docmd.c:8825
    #7 0x557b66234f4a in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:8788
    #8 0x557b662347ee in ex_normal /home/fuzz/vim/src/ex_docmd.c:8706
    #9 0x557b66210f7c in do_one_cmd /home/fuzz/vim/src/ex_do
    #10 0x557b662081d8 in do_cmdline /home/fuzz/vim/src/ex_
    #11 0x557b6652d77c in do_source_ext /home/fuzz/vim/src/scriptfile.c:166
```

```
    #12 0x557b6652e9b1 in do_source /home/fuzz/vim/src/scriptfile.c:1808
    #13 0x557b6652b46f in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #14 0x557b6652b4d4 in ex_source /home/fuzz/vim/src/scriptfile.c:1189

    #15 0x557b66210f7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #16 0x557b662081d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #17 0x557b66206572 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #18 0x557b6680b8be in exe_commands /home/fuzz/vim/src/main.c:3139
    #19 0x557b66804a27 in vim_main2 /home/fuzz/vim/src/main.c:781
    #20 0x557b668042df in main /home/fuzz/vim/src/main.c:432
    #21 0x7f8bddff7082 in __libc_start_main ../csu/libc-start.c:308
    #22 0x557b66085e4d in _start (/home/fuzz/vim/src/vim+0x13ae4d)

0x6020000063f2 is located 0 bytes to the right of 2-byte region [0x60200006
allocated by thread T0 here:
    #0 0x7f8bde48e808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x557b6608628a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x557b6608607b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x557b6637d267 in coladvance2 /home/fuzz/vim/src/misc2.c:236
    #4 0x557b6637c02c in coladvance_force /home/fuzz/vim/src/misc2.c:58
    #5 0x557b663e59d0 in op_replace /home/fuzz/vim/src/ops.c:1203
    #6 0x557b663fdce4 in do_pending_operator /home/fuzz/vim/src/ops.c:4200
    #7 0x557b663b3dce in normal_cmd /home/fuzz/vim/src/normal.c:959
    #8 0x557b6623518b in exec_normal /home/fuzz/vim/src/ex_docmd.c:8825
    #9 0x557b66234f4a in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:8788
    #10 0x557b662347ee in ex_normal /home/fuzz/vim/src/ex_docmd.c:8706
    #11 0x557b66210f7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #12 0x557b662081d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #13 0x557b6652d77c in do_source_ext /home/fuzz/vim/src/scriptfile.c:166
    #14 0x557b6652e9b1 in do_source /home/fuzz/vim/src/scriptfile.c:1808
    #15 0x557b6652b46f in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #16 0x557b6652b4d4 in ex_source /home/fuzz/vim/src/scriptfile.c:1189
    #17 0x557b66210f7c in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #18 0x557b662081d8 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #19 0x557b66206572 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #20 0x557b6680b8be in exe_commands /home/fuzz/vim/src/main.c:3139
    #21 0x557b66804a27 in vim_main2 /home/fuzz/vim/src/main.c:781
    #22 0x557b668042df in main /home/fuzz/vim/src/main.c:432
    #23 0x7f8bddff7082 in __libc_start_main ../csu/libc-start

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim/src/mbyte.c:
```

```
Shadow bytes around the buggy address:
  0x0c047fff8c20: fa fa 03 fa fa fa 03 fa fa fa 03 fa fa fa fd fa
  0x0c047fff8c30: fa fa 03 fa fa fa fd fa fa fa 00 00 fa fa 01 fa

  0x0c047fff8c40: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 02 fa
  0x0c047fff8c50: fa fa 03 fa fa fa 03 fa fa fa 04 fa fa fa 01 fa
  0x0c047fff8c60: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 03 fa
=>0x0c047fff8c70: fa fa fd fa fa fa 02 fa fa fa 02 fa fa fa[02]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
  0x0c047fff8cb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8cc0: 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
==130015==ABORTING
```

poc download url: https://github.com/Janette88/vim/blob/main/poc6_hbo.dat

Impact

This vulnerabilities are capable of crashing software, Modify Memory, and possible remote

execution.

CVE
CVE-2022-3234
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,279 times.

We are processing your report and will contact the vim team within 24 hours. 2 months ago

We have contacted a member of the vim team and are waiting to hear bac

Bram Moolenaar validated this vulnerability 2 months ago

I can reproduce the problem.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 2 months ago Maintainer

Fixed with patch 9.0.0483

Bram Moolenaar marked this as fixed in 9.0.0483 with commit c24991 2 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation