Buffer Over-read in function utfc_ptr2len in vim/vim

0

Valid Reported on Apr 28th 2022

Description

Buffer Over-read in function utfc_ptr2len at mbyte.c:2113

vim version

```
git log
commit 5a8fad32ea9c075f045b37d6c7739891d458f82b (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /mnt/share/max/fuzz/poc/vim/poc_
==================================================================
==18557==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000(
READ of size 1 at 0x6020000077b2 thread T0
    #0 0xa3df45 in utfc_ptr2len /home/fuzz/fuzz/vim/vim/src/mbyte.c:2113:15
    #1 0xb34578 in get_visual_text /home/fuzz/fuzz/vim/vim/src/normal.c:367
    #2 0xb31086 in nv_ident /home/fuzz/fuzz/vim/vim/src/normal.c:3469:23
    #3 0xb1a341 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #4 0x80ebde in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8757:
    #5 0x80e408 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8
    #6 0x80dfb9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8638:6
    #7 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #8 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #9 0x11503df in call_user_func /home/fuzz/fuzz/vim/vim/src/userfunc.c:2
    #10 0x114c4bd in call_user_func_check /home/fuzz/fuzz/vim/vim/src/userf
    #11 0x1146844 in call_func /home/fuzz/fuzz/vim/vim/src/
    #12 0x1143bef in get_func_tv /home/fuzz/fuzz/vim/vim/src/
    #13 0x11764b6 in ex_call /home/fuzz/fuzz/vim/vim/src/userfunc.c:5513:6
```

```
    #14 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #15 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #16 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c
    #17 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #18 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #19 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #20 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #21 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #22 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #23 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
    #24 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #25 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #26 0x7fcb54965082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #27 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x6020000077b2 is located 0 bytes to the right of 2-byte region [0x60200000
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 0xf85f7d in vim_strnsave /home/fuzz/fuzz/vim/vim/src/strings.c:44:9
    #4 0xa75d55 in ml_replace_len /home/fuzz/fuzz/vim/vim/src/memline.c:344
    #5 0xa75a22 in ml_replace /home/fuzz/fuzz/vim/vim/src/memline.c:3404:12
    #6 0x7af7f1 in ex_substitute /home/fuzz/fuzz/vim/vim/src/ex_cmds.c:4670
    #7 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #8 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #9 0x11503df in call_user_func /home/fuzz/fuzz/vim/vim/src/userfunc.c:2
    #10 0x114c4bd in call_user_func_check /home/fuzz/fuzz/vim/vim/src/userf
    #11 0x1146844 in call_func /home/fuzz/fuzz/vim/vim/src/userfunc.c:3612
    #12 0x1143bef in get_func_tv /home/fuzz/fuzz/vim/vim/src/userfunc.c:183
    #13 0x11764b6 in ex_call /home/fuzz/fuzz/vim/vim/src/userfunc.c:5513:6
    #14 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #15 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #16 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c
    #17 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #18 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #19 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #20 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #21 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #22 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
```

```
    #23 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
    #24 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #25 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12

    #26 0x7fcb54965082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/vim/src
Shadow bytes around the buggy address:
  0x0c047fff8ea0: fa fa 02 fa fa fa 02 fa fa fa fd fa fa fa fd fa
  0x0c047fff8eb0: fa fa 05 fa fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c047fff8ec0: fa fa fd fa fa fa 02 fa fa fa 02 fa fa fa 02 fa
  0x0c047fff8ed0: fa fa fd fa fa fa fd fa fa fa 01 fa fa fa 02 fa
  0x0c047fff8ee0: fa fa 02 fa fa fa fd fa fa fa fd fa fa fa 01 fa
=>0x0c047fff8ef0: fa fa fd fa fa fa[02]fa fa fa 00 04 fa fa 01 fa
  0x0c047fff8f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8f40: 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
==18557==ABORTING
```

poc_h8_s.dat

Impact

This vulnerabilities are capable of crashing software, modify memory, and possible remote execution

CVE
CVE-2022-1735
(Published)

Vulnerability Type
CWE-120: Classic Buffer Overflow

Severity
Medium (6.6)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar
@brammool
maintainer

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

The POC file looks like a bunch of random bytes. Please reduce this to the minimum to reproduce the problem.

We have sent a second follow up to the **vim** team. We will try again in 10 days. 7 months ago

TDHX ICS Security modified the report 6 months ago

TDHX 6 months ago — Researcher

I cannot reproduce the orignal issue either, but found another location with the same issue, so the report is updated to the new location with new poc file, hope you can reproduce it.

Bram Moolenaar 6 months ago — Maintainer

With this POC I can reproduce the error. I can even simplify the POC a bit more, avoiding the function call and removing some commands.
I'll make a fix.

Bram Moolenaar validated this vulnerability 6 months ago

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 6 months ago — Maintainer

Fixed in patch 8.2.4969

Bram Moolenaar marked this as fixed in 8.2 with commit 7ce5b2 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation