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

0

Valid Reported on Jun 29th 2022

Description

Heap-based Buffer Overflow in function utfc_ptr2len at mbyte.c:2113

vim version

```
git log
commit 75417d960bd17a5b701cfb625b8864dacaf0cc39 (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_hbor3_s.dat -c :qa
==================================================================
==3951097==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 1 at 0x6020000086d4 thread T0
    #0 0xa43695 in utfc_ptr2len /home/fuzz/fuzz/vim/afl/src/mbyte.c:2113:15
    #1 0xb3a298 in get_visual_text /home/fuzz/fuzz/vim/afl/src/normal.c:368
    #2 0xb78b8f in nv_zg_zw /home/fuzz/fuzz/vim/afl/src/normal.c:2615:26
    #3 0xb6481b in nv_zet /home/fuzz/fuzz/vim/afl/src/normal.c:3001:7
    #4 0xb1fe8f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #5 0x81539e in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812:
    #6 0x814bc8 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8
    #7 0x814779 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:6
    #8 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex
    #9 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/e
    #10 0x1159f0c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
```

```
    #11 0x1155ffd in call_user_func_check /home/fuzz/fuzz/vim/afl/src/userf
    #12 0x11503a4 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3613:
    #13 0x114d743 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183

    #14 0x1180e6a in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5594:6
    #15 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #16 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #17 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #18 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #19 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #20 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #21 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #22 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #23 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #24 0x1424092 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #25 0x142022b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #26 0x141573d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #27 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #28 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x6020000086d4 is located 0 bytes to the right of 4-byte region [0x60200000
allocated by thread T0 here:
    #0 0x499cbd in malloc (/home/fuzz/fuzz/vim/afl/src/vim+0x499cbd)
    #1 0x4cb392 in lalloc /home/fuzz/fuzz/vim/afl/src/alloc.c:246:11
    #2 0x4cb27a in alloc /home/fuzz/fuzz/vim/afl/src/alloc.c:151:12
    #3 0x54e3a4 in ins_str /home/fuzz/fuzz/vim/afl/src/change.c:1176:12
    #4 0x6975e4 in insertchar /home/fuzz/fuzz/vim/afl/src/edit.c:2249:2
    #5 0x68fa79 in insert_special /home/fuzz/fuzz/vim/afl/src/edit.c:2038:2
    #6 0x675137 in edit /home/fuzz/fuzz/vim/afl/src/edit.c:1359:3
    #7 0xb6a9cc in invoke_edit /home/fuzz/fuzz/vim/afl/src/normal.c:7035:9
    #8 0xb4d9bd in nv_edit /home/fuzz/fuzz/vim/afl/src/normal.c:7005:2
    #9 0xb1fe8f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #10 0x81539e in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812
    #11 0x814bc8 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:
    #12 0x814779 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:6
    #13 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #14 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #15 0x1159f0c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
    #16 0x1155ffd in call_user_func_check /home/fuzz/fuzz/vim/afl/src/
    #17 0x11503a4 in call_func /home/fuzz/fuzz/vim/afl/src/
    #18 0x114d743 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
```

```
    #19 0x1180e6a in ex_call /home/fuzz/fuzz/vim/afl/src/usercmd.c:5594:6
    #20 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #21 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1

    #22 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #23 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #24 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #25 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #26 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #27 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #28 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #29 0x1424092 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/afl/src
Shadow bytes around the buggy address:
  0x0c047fff9080: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff9090: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd
  0x0c047fff90a0: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd
  0x0c047fff90b0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff90c0: fa fa fd fd fa fa fd fa fa fa 01 fa fa fa 00 00
=>0x0c047fff90d0: fa fa 01 fa fa fa fd fa fa fa[04]fa fa fa fd fa
  0x0c047fff90e0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff90f0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff9100: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff9110: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff9120: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fd
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
  ==3951097==ABORTING
```

poc_hbor3_s.dat

Impact

This vulnerability is capable of crashing software, modify memory, and possible remote execution.

CVE
CVE-2022-2284
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

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 681 times.

We are processing your report and will contact the **vim** team within 24 hours. 5 months ago

We have contacted a member of the **vim** team and are waiting to hear back 5 months ago

Bram Moolenaar 5 months ago Maintainer

I can reproduce it. Took some effort to bring the POC into a simpler version.

Bram Moolenaar validated this vulnerability 5 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 5 months ago Maintainer

Fixed with patch 9.0.0017

Bram Moolenaar marked this as fixed in **9.0** with commit **3d51ce** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation