Out-of-bounds Read in function utf_ptr2char in vim/vim

0

Valid Reported on Jul 5th 2022

Description

Out-of-bounds Read in function utf_ptr2char at mbyte.c:1794

vim version

```
git log
commit 324478037923feef1eb8a771648e38ade9e5e05a (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_obr5_s.dat -c :qa!
==================================================================
==11944==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000(
READ of size 1 at 0x6020000062f2 thread T0
    #0 0xa46868 in utf_ptr2char /home/fuzz/fuzz/vim/afl/src/mbyte.c:1794:9
    #1 0xd996cc in find_match_text /home/fuzz/fuzz/vim/afl/src/./regexp_nfa
    #2 0xd97afb in nfa_regexec_both /home/fuzz/fuzz/vim/afl/src/./regexp_nf
    #3 0xcfa1f5 in nfa_regexec_nl /home/fuzz/fuzz/vim/afl/src/./regexp_nfa.
    #4 0xcf64ad in vim_regexec_string /home/fuzz/fuzz/vim/afl/src/regexp.c:
    #5 0xcf6cf9 in vim_regexec /home/fuzz/fuzz/vim/afl/src/regexp.c:2931:12
    #6 0x541a4b in fname_match /home/fuzz/fuzz/vim/afl/src/buffer.c:2954:6
    #7 0x51d9ca in buflist_match /home/fuzz/fuzz/vim/afl/src/buffer.c:2928:
    #8 0x51836b in buflist_findpat /home/fuzz/fuzz/vim/afl/src/buffer.c:264
    #9 0x7dd3d1 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2535:1
    #10 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/
    #11 0xe5c8fe in do_source_ext /home/fuzz/fuzz/vim/afl/src/
    #12 0xe58940 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:115
```

```
    #13 0xe583de in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #14 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #15 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #16 0xe5c8fe in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c
    #17 0xe59396 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #18 0xe58cd3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #19 0xe583de in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #20 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #21 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #22 0x7cf591 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #23 0x1427482 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #24 0x142361b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #25 0x1418b2d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #26 0x7f885dc42082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #27 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x6020000062f2 is located 0 bytes to the right of 2-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 0xf90e26 in vim_strsave /home/fuzz/fuzz/vim/afl/src/strings.c:27:9
    #4 0x50f9a3 in buflist_new /home/fuzz/fuzz/vim/afl/src/buffer.c:2105:18
    #5 0x5289f2 in buflist_add /home/fuzz/fuzz/vim/afl/src/buffer.c:3605:11
    #6 0x4d0f00 in alist_add /home/fuzz/fuzz/vim/afl/src/arglist.c:206:6
    #7 0x4d0aaa in alist_set /home/fuzz/fuzz/vim/afl/src/arglist.c:173:6
    #8 0x4d2ccf in do_arglist /home/fuzz/fuzz/vim/afl/src/arglist.c:484:6
    #9 0x4d56f7 in ex_next /home/fuzz/fuzz/vim/afl/src/arglist.c:751:10
    #10 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #11 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #12 0xe5c8fe in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c
    #13 0xe59396 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #14 0xe58cd3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #15 0xe583de in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #16 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #17 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #18 0x7cf591 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #19 0x1427482 in exe_commands /home/fuzz/fuzz/vim/afl/src/
    #20 0x142361b in vim_main2 /home/fuzz/fuzz/vim/afl/src/
    #21 0x1418b2d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
```

```
    #22 0x7f885dc42082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/afl/src

Shadow bytes around the buggy address:
  0x0c047fff8c00: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8c10: fa fa fd fa fa fa fd fa fa fa 00 00 fa fa 00 00
  0x0c047fff8c20: fa fa 05 fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8c30: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8c40: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fd
=>0x0c047fff8c50: fa fa 00 03 fa fa fd fa fa fa 02 fa fa fa[02]fa
  0x0c047fff8c60: fa fa 01 fa fa fa 05 fa fa fa 00 04 fa fa 01 fa
  0x0c047fff8c70: fa fa 01 fa fa fa 01 fa fa fa 01 fa fa fa 07 fa
  0x0c047fff8c80: fa fa 03 fa fa fa 00 06 fa fa 00 04 fa fa 01 fa
  0x0c047fff8c90: fa fa 01 fa fa fa 03 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff8ca0: fa fa 01 fa fa fa 01 fa fa fa 01 fa fa fa 01 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
==11944==ABORTING
```


poc_obr5_s.dat

poc_obj_3.dat

Impact

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

CVE
CVE-2022-2581
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

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 539 times.

Chat with us

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

We have sent a follow up to the **vim** team. We will try again in 7 days. 5 months ago

We have sent a second follow up to the **vim** team. We will try again in 10 days. 4 months ago

We have sent a third and final follow up to the **vim** team. This report is now considered stale. 4 months ago

Bram Moolenaar validated this vulnerability 4 months ago

I can reproduce the problem. Turning the POC into a regression test is difficult.

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 4 months ago Maintainer

Fixed with patch 9.0.0105

Bram Moolenaar marked this as fixed in **9.0.0104** with commit **f50940** 4 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation