Heap-based Buffer Overflow in function utf_ptr2char in vim/vim

0

Valid Reported on Jun 20th 2022

Description

Heap-based Buffer Overflow in function utf_ptr2char at mbyte.c:1794

vim version

```
git log
commit e366ed4f2c6fa8cb663f1b9599b39d57ddbd8a2a (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_
==================================================================
==10679==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6210000
READ of size 1 at 0x621000013d02 thread T0
    #0 0xa454c8 in utf_ptr2char /home/fuzz/fuzz/vim/afl/src/mbyte.c:1794:9
    #1 0xaab423 in gchar_pos /home/fuzz/fuzz/vim/afl/src/misc1.c:523:9
    #2 0x10a9e85 in findsent /home/fuzz/fuzz/vim/afl/src/textobject.c:50:6
    #3 0xa1aa3e in getmark_buf_fnum /home/fuzz/fuzz/vim/afl/src/mark.c:354:
    #4 0xa1bcaf in getmark /home/fuzz/fuzz/vim/afl/src/mark.c:293:12
    #5 0x7eb4ec in get_address /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:4371:
    #6 0x7f0327 in parse_cmd_address /home/fuzz/fuzz/vim/afl/src/ex_docmd.c
    #7 0x7d3adb in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:1940:6
    #8 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex
    #9 0xe5928e in do_source_ext /home/fuzz/fuzz/vim/afl/sr
    #10 0xe552d0 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:115
```

```
    #11 0xe54d6e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #12 0x7dd349 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #13 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1

    #14 0xe5928e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #15 0xe55d26 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #16 0xe55663 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #17 0xe54d6e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #18 0x7dd349 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #19 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #20 0x7cee81 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #21 0x1423142 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #22 0x141f2db in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #23 0x14147ed in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #24 0x7ffff7bed082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #25 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x621000013d02 is located 2 bytes to the right of 4096-byte region [0x62100
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 0x142ca45 in mf_alloc_bhdr /home/fuzz/fuzz/vim/afl/src/memfile.c:884
    #4 0x142b857 in mf_new /home/fuzz/fuzz/vim/afl/src/memfile.c:375:26
    #5 0xa61068 in ml_new_data /home/fuzz/fuzz/vim/afl/src/memline.c:4080:1
    #6 0xa5fa11 in ml_open /home/fuzz/fuzz/vim/afl/src/memline.c:394:15
    #7 0x501c9a in open_buffer /home/fuzz/fuzz/vim/afl/src/buffer.c:186:9
    #8 0x142098c in create_windows /home/fuzz/fuzz/vim/afl/src/main.c:2902:
    #9 0x141ec5a in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:711:5
    #10 0x14147ed in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #11 0x7ffff7bed082 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:
  0x0c427fffa750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa790: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fffa7a0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c427fffa7c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

  0x0c427fffa7f0: 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
==10679==ABORTING
```

poc_hbo3_s.dat

Impact

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

CVE
CVE-2022-2182
(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 735 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 validated this vulnerability 5 months ago

I can easily reproduce the problem.

TDHX ICS Security has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

Bram Moolenaar 5 months ago Maintainer

Fixed with patch 8.2.5150

Bram Moolenaar marked this as fixed in 8.2 with commit f7c7c3 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation