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

0

Valid Reported on May 22nd 2022

Description

Heap-based Buffer Overflow in function utf_head_off at mbyte.c:3872

vim Version

```
git log
commit 68e64d2c1735f2a39afa8a0475ae29bedb116684 (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S poc_h6_s.dat -c :qa!
==================================================================
==48342==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000(
READ of size 1 at 0x60200000860f thread T0
    #0 0xa467fc in utf_head_off /home/fuzz/fuzz/vim/vim/src/mbyte.c:3872:9
    #1 0xe02062 in do_put /home/fuzz/fuzz/vim/vim/src/register.c:2223:7
    #2 0xb6dbb3 in nv_put_opt /home/fuzz/fuzz/vim/vim/src/normal.c:7351:2
    #3 0xb55466 in nv_brackets /home/fuzz/fuzz/vim/vim/src/normal.c:4514:2
    #4 0xb1fed1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #5 0x813d5e in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:
    #6 0x813588 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8
    #7 0x813139 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #8 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #9 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex
    #10 0xe57a2c in do_source_ext /home/fuzz/fuzz/vim/vim/s
    #11 0xe54486 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
```

```
    #12 0xe53dbc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #13 0xe5349e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #14 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:

    #15 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #16 0x7cdc51 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #17 0x1423782 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #18 0x141f91b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #19 0x1415015 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #20 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #21 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x60200000860f is located 1 bytes to the left of 1-byte region [0x602000008
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 0xf8c1f6 in vim_strsave /home/fuzz/fuzz/vim/vim/src/strings.c:27:9
    #4 0xdf2757 in get_register /home/fuzz/fuzz/vim/vim/src/register.c:310:
    #5 0xb6cfa7 in nv_put_opt /home/fuzz/fuzz/vim/vim/src/normal.c:7307:10
    #6 0xb55466 in nv_brackets /home/fuzz/fuzz/vim/vim/src/normal.c:4514:2
    #7 0xb1fed1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #8 0x813d5e in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:
    #9 0x813588 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8
    #10 0x813139 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #11 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
    #12 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #13 0xe57a2c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #14 0xe54486 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #15 0xe53dbc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #16 0xe5349e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #17 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
    #18 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #19 0x7cdc51 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #20 0x1423782 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #21 0x141f91b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #22 0x1415015 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #23 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/
Shadow bytes around the buggy address:
```

```
  0x0c047fff9070: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff9080: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff9090: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa

  0x0c047fff90a0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff90b0: fa fa fd fa fa fa 02 fa fa fa 04 fa fa fa 01 fa
=>0x0c047fff90c0: fa[fa]01 fa fa fa 02 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff90d0: fa fa 01 fa fa fa 02 fa fa fa fd fd fa fa fd fa
  0x0c047fff90e0: fa fa fd fd fa fa 00 04 fa fa 00 00 fa fa 00 04
  0x0c047fff90f0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fa fa
  0x0c047fff9100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9110: 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
==48342==ABORTING
```

poc_h6_s.dat

Impact

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

CVE

CVE-2022-1886
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.1)

Registry
Other

Affected Version
<=8.2.5006

Visibility
Public

Status
Fixed

Found by

TDHX ICS Security

@unkn0wne

unranked

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 860 times.

We are processing your report and will contact the **vim** team within 24 hours. 6 months ago

TDHX ICS Security modified the report 6 months ago

TDHX ICS Security modified the report 6 months ago

We have contacted a member of the **vim** team and are waiting to hear back 6 months ago

Bram Moolenaar 6 months ago

This POC is much too long. Please reduce to the essential.

TDHX 6 months ago Researcher

OK, I've simplified POC.
https://github.com/Unkn0wne/Poc/blob/bc9aea2ac92730862cb0500c8b28e0ceb3fc6cdb/vim/poc_h14_s.dat

Bram Moolenaar 6 months ago

Thank you. I could reproduce the problem and find out why it happens. I simplified the POC a bit more to use as a test.
Fixed in Patch 8.2.5016

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 marked this as fixed in **8.2** with commit **2a585c** 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation