Out-of-bounds write in function append_command in vim/vim

2

Valid Reported on Jun 3rd 2022

Description

Out-of-bounds write in function append_command at ex_docmd.c:3447

vim version

```
git log
commit bfaa24f95343af9c058696644375d04e660f1b00 (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_obw6_s.dat -c :qa!
==================================================================
==3497672==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61900
WRITE of size 3 at 0x619000000e81 thread T0
    #0 0x4848d8 in strcat (/home/fuzz/fuzz-vim/vim/src/vim+0x4848d8)
    #1 0x816a2d in append_command /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:34
    #2 0x7de9e5 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2619:6
    #3 0x7ca815 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #4 0x7c6699 in do_exmode /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:517:6
    #5 0xb5502a in nv_exmode /home/fuzz/fuzz/vim/vim/src/normal.c:3155:2
    #6 0xb2220f in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:941:5
    #7 0x81591e in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8792:
    #8 0x815148 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/s
    #9 0x814cf9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex
    #10 0x7ddaa9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
```

```
    #11 0x7ca815 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #12 0xe5aadc in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #13 0xe57536 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801

    #14 0xe56e6c in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #15 0xe5654e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #16 0x7ddaa9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #17 0x7ca815 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #18 0x7cf4b1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #19 0x1426b42 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #20 0x1422cdb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #21 0x14183d5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #22 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #23 0x41ea6d in _start (/home/fuzz/fuzz-vim/vim/src/vim+0x41ea6d)

0x619000000e81 is located 0 bytes to the right of 1025-byte region [0x61900
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 0x141843a in common_init /home/fuzz/fuzz/vim/vim/src/main.c:914:19
    #4 0x1417924 in main /home/fuzz/fuzz/vim/vim/src/main.c:185:5
    #5 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/c

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz-vim/vim/sr
Shadow bytes around the buggy address:
  0x0c327fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff81d0:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8220: fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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
  ==3497672==ABORTING
```

poc_obw6_s.dat

Impact

This may result in corruption of sensitive information, a crash, or code execution among other things.

CVE
CVE-2022-2000
(Published)

Vulnerability Type
CWE-787: Out-of-bounds Write

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 1,303 times.

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

I can reproduce it. I can use the POC for a regression test.

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 **44a3f3** 6 months

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Sign in to join this conversation