huntr

Buffer Over-read in function put_on_cmdline in vim/vim

0

✓ Valid   Reported on Jun 20th 2022

Description

Buffer Over-read in function put_on_cmdline at ex_getln.c:3540

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_
=================================================================
==12124==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b0000
READ of size 2 at 0x60b00000092f thread T0
    #0 0x4994be in __asan_memmove (/home/fuzz/fuzz/vim/afl/src/vim+0x4994be
    #1 0x85eab2 in put_on_cmdline /home/fuzz/fuzz/vim/afl/src/ex_getln.c:35
    #2 0x855bb7 in getcmdline_int /home/fuzz/fuzz/vim/afl/src/ex_getln.c:24
    #3 0x84ac7e in getcmdline /home/fuzz/fuzz/vim/afl/src/ex_getln.c:1569:1
    #4 0xb49478 in nv_search /home/fuzz/fuzz/vim/afl/src/normal.c:4155:22
    #5 0xb1f8df in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #6 0x814fee in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8809:
    #7 0x814818 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8
    #8 0x8143c9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8690:6
    #9 0x7dd349 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #10 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/
    #11 0xe5928e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #12 0xe55d26 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
```

Chat with us

```
    #12 0xe55d26 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:180
    #13 0xe55663 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #14 0xe54d6e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #15 0x7dd349 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #16 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #17 0x7cee81 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #18 0x1423142 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #19 0x141f2db in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #20 0x14147ed in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #21 0x7ffff7bed082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #22 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x60b00000092f is located 1 bytes to the left of 100-byte region [0x60b0000
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 0x85cc15 in alloc_cmdbuff /home/fuzz/fuzz/vim/afl/src/ex_getln.c:329
    #4 0x866f10 in init_ccline /home/fuzz/fuzz/vim/afl/src/ex_getln.c:1523
    #5 0x84b4d1 in getcmdline_int /home/fuzz/fuzz/vim/afl/src/ex_getln.c:16
    #6 0x84ac7e in getcmdline /home/fuzz/fuzz/vim/afl/src/ex_getln.c:1569:1
    #7 0xb49478 in nv_search /home/fuzz/fuzz/vim/afl/src/normal.c:4155:22
    #8 0xb1f8df in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #9 0x814fee in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8809
    #10 0x814818 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c
    #11 0x8143c9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8690:6
    #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-SzI

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz/vim/afl/sr
Shadow bytes around the buggy address:
  0x0c167fff80d0: fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa
  0x0c167fff80e0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd

  0x0c167fff80f0: fd fa fa fa fa fa fa fa fa fa fd fd fd fd fd fd
  0x0c167fff8100: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa
  0x0c167fff8110: fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa
=>0x0c167fff8120: fa fa fa fa fa[fa]00 00 00 00 00 00 00 00 00 00
  0x0c167fff8130: 00 00 04 fa fa fa fa fa fa fa fa fa 00 00 00 00
  0x0c167fff8140: 00 00 00 00 00 00 00 00 04 fa fa fa fa fa fa fa
  0x0c167fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8170: 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
==12124==ABORTING
```

poc_bor2_s.dat

Impact

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

CVE
CVE-2022-2175
(Published)

Vulnerability Type
CWE-126: Buffer Over-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 866 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 bac

Chat with us

Bram Moolenaar 5 months ago Maintainer

Bram Moolenaar 5 months ago Maintainer

I can reproduce it. The POC can be shortened by expanding the mapping and removing some characters.

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 8.2.5148

Bram Moolenaar marked this as fixed in 8.2 with commit 6046ad 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation