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

0

Valid Reported on Apr 27th 2022

Description

Heap-based Buffer Overflow in function cmdline_erase_chars at ex_getln.c:1085

POC

```
./vim -u NONE -X -Z -e -s -S ./poc_h1.dat -c :qa!
==================================================================
==3840814==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b0
READ of size 1 at 0x60b00000087f thread T0
    #0 0x886659 in cmdline_erase_chars /home/fuzz/vim/vim-master/src/ex_get
    #1 0x86c472 in getcmdline_int /home/fuzz/vim/vim-master/src/ex_getln.c:
    #2 0x86483e in getcmdline /home/fuzz/vim/vim-master/src/ex_getln.c:1571
    #3 0x872ce6 in getexline /home/fuzz/vim/vim-master/src/ex_getln.c:2853:
    #4 0x7e3982 in do_cmdline /home/fuzz/vim/vim-master/src/ex_docmd.c:875:
    #5 0xb70283 in nv_colon /home/fuzz/vim/vim-master/src/normal.c:3191:19
    #6 0xb45243 in normal_cmd /home/fuzz/vim/vim-master/src/normal.c:930:5
    #7 0x82eefe in exec_normal /home/fuzz/vim/vim-master/src/ex_docmd.c:875
    #8 0x82e728 in exec_normal_cmd /home/fuzz/vim/vim-master/src/ex_docmd.c
    #9 0x82e2d9 in ex_normal /home/fuzz/vim/vim-master/src/ex_docmd.c:8634:
    #10 0x7f7a25 in do_one_cmd /home/fuzz/vim/vim-master/src/ex_docmd.c:256
    #11 0x7e49a5 in do_cmdline /home/fuzz/vim/vim-master/src/ex_docmd.c:992
    #12 0xe88e0c in do_source_ext /home/fuzz/vim/vim-master/src/scriptfile.
    #13 0xe85866 in do_source /home/fuzz/vim/vim-master/src/scriptfile.c:18
    #14 0xe8519c in cmd_source /home/fuzz/vim/vim-master/src/scriptfile.c:1
    #15 0xe8487e in ex_source /home/fuzz/vim/vim-master/src/scriptfile.c:12
    #16 0x7f7a25 in do_one_cmd /home/fuzz/vim/vim-master/src/ex_docmd.c:256
    #17 0x7e49a5 in do_cmdline /home/fuzz/vim/vim-master/sr
    #18 0x7e95f1 in do_cmdline_cmd /home/fuzz/vim/vim-maste
    #19 0x144d0a2 in exe_commands /home/fuzz/vim/vim-master/src/main.c:3108
```

```
    #20 0x144922d in vim_main2 /home/fuzz/vim/vim-master/src/main.c:780:2
    #21 0x143e484 in main /home/fuzz/vim/vim-master/src/main.c:432:12
    #22 0x7ffff78260b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #23 0x41fe5d in _start (/home/fuzz/fuzz-vim/vim-master/src/vim+0x41fe5d

0x60b00000087f is located 1 bytes to the left of 100-byte region [0x60b00000
allocated by thread T0 here:
    #0 0x49b0bd in malloc (/home/fuzz/fuzz-vim/vim-master/src/vim+0x49b0bd)
    #1 0x4cc79a in lalloc /home/fuzz/vim/vim-master/src/alloc.c:246:11
    #2 0x4cc67a in alloc /home/fuzz/vim/vim-master/src/alloc.c:151:12
    #3 0x876aa5 in alloc_cmdbuff /home/fuzz/vim/vim-master/src/ex_getln.c:3
    #4 0x8807c0 in init_ccline /home/fuzz/vim/vim-master/src/ex_getln.c:152
    #5 0x865080 in getcmdline_int /home/fuzz/vim/vim-master/src/ex_getln.c:
    #6 0x86483e in getcmdline /home/fuzz/vim/vim-master/src/ex_getln.c:1571
    #7 0x872ce6 in getexline /home/fuzz/vim/vim-master/src/ex_getln.c:2853:
    #8 0x7e3982 in do_cmdline /home/fuzz/vim/vim-master/src/ex_docmd.c:875:
    #9 0xb70283 in nv_colon /home/fuzz/vim/vim-master/src/normal.c:3191:19
    #10 0xb45243 in normal_cmd /home/fuzz/vim/vim-master/src/normal.c:930:5
    #11 0x82eefe in exec_normal /home/fuzz/vim/vim-master/src/ex_docmd.c:87
    #12 0x82e728 in exec_normal_cmd /home/fuzz/vim/vim-master/src/ex_docmd.
    #13 0x82e2d9 in ex_normal /home/fuzz/vim/vim-master/src/ex_docmd.c:8634
    #14 0x7f7a25 in do_one_cmd /home/fuzz/vim/vim-master/src/ex_docmd.c:256
    #15 0x7e49a5 in do_cmdline /home/fuzz/vim/vim-master/src/ex_docmd.c:992
    #16 0xe88e0c in do_source_ext /home/fuzz/vim/vim-master/src/scriptfile.
    #17 0xe85866 in do_source /home/fuzz/vim/vim-master/src/scriptfile.c:18
    #18 0xe8519c in cmd_source /home/fuzz/vim/vim-master/src/scriptfile.c:1
    #19 0xe8487e in ex_source /home/fuzz/vim/vim-master/src/scriptfile.c:12
    #20 0x7f7a25 in do_one_cmd /home/fuzz/vim/vim-master/src/ex_docmd.c:256
    #21 0x7e49a5 in do_cmdline /home/fuzz/vim/vim-master/src/ex_docmd.c:992
    #22 0x7e95f1 in do_cmdline_cmd /home/fuzz/vim/vim-master/src/ex_docmd.c
    #23 0x144d0a2 in exe_commands /home/fuzz/vim/vim-master/src/main.c:3108
    #24 0x144922d in vim_main2 /home/fuzz/vim/vim-master/src/main.c:780:2
    #25 0x143e484 in main /home/fuzz/vim/vim-master/src/main.c:432:12
    #26 0x7ffff78260b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim/vim-master/s
Shadow bytes around the buggy address:
  0x0c167fff80b0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c167fff80c0: 00 00 00 00 00 fa fa fa fa fa fa fa fa fa fa
  0x0c167fff80d0: 00 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa
```

```
  0x0c167fff80e0: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c167fff80f0: 00 fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00
=>0x0c167fff8100: 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa[fa]

  0x0c167fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 04 fa fa fa
  0x0c167fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8150: 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
==3840814==ABORTING
```

poc_h1.dat

Impact

This vulnerabilities are capable of crashing software, modify memory, and possible remote execution

CVE
CVE-2022-1619
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (6.1)

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 1,268 times.

We are processing your report and will contact the **vim** team within 24 hours. 7 months ago

TDHX ICS Security modified the report 7 months ago

We have contacted a member of the **vim** team and are waiting to hear back 7 months ago

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

Bram Moolenaar 7 months ago Maintainer

The POC file is too long. I tried deleting a few characters and the problem persists. Please reduce the POC to the minimum to reproduce the problem.

TDHX 7 months ago Researcher

Try to reduce the POC to poc_h1_s.dat

Reproduced the problem with the reduced POC as following:

```
# ./vim -u NONE -X -Z -e -s -S /mnt/share/max/fuzz/poc/vim/poc_h1_s.dat -c :qa!
=================================================================
==75948==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b00000087f at pc
READ of size 1 at 0x60b00000087f thread T0
    #0 0x886659 in cmdline_erase_chars /home/fuzz/vim-master/src/ex_getln.c:1085:22
    #1 0x86c472 in getcmdline_int /home/fuzz/vim-master/src/ex_getln.c:2029:12
    #2 0x86483e in getcmdline /home/fuzz/vim-master/src/ex_getln.c:1571:12
    #3 0x872ce6 in getexline /home/fuzz/vim-master/src/ex_getln.c:2853:12
    #4 0x7e3982 in do_cmdline /home/fuzz/vim-master/src/ex_docmd.c:875:46
    #5 0xb70283 in nv_colon /home/fuzz/vim-master/src/normal.c:3191:19
    #6 0xb45243 in normal_cmd /home/fuzz/vim-master/src/normal.c:930:5
    #7 0x82eefe in exec_normal /home/fuzz/vim-master/src/ex_docmd.c:8753:6
    #8 0x82e728 in exec_normal_cmd /home/fuzz/vim-master/src/ex_docmd.c:8716:5
    #9 0x82e2d9 in ex_normal /home/fuzz/vim-master/src/ex_docmd.c:8634:6
    #10 0x7f7a25 in do_one_cmd /home/fuzz/vim-master/src/ex_docmd.c:2567:2
    #11 0x7e49a5 in do_cmdline /home/fuzz/vim-master/src/ex_docmd.c:992:17
    #12 0xe88e0c in do_source_ext /home/fuzz/vim-master/src/scriptfile.c:1674:5
    #13 0xe85866 in do_source /home/fuzz/vim-master/src/scriptfile.c:1801:12
    #14 0xe8519c in cmd_source /home/fuzz/vim-master/src/scriptfile.c:1174:14
    #15 0xe8487e in ex_source /home/fuzz/vim-master/src/scriptfile.c:1200:2
    #16 0x7f7a25 in do_one_cmd /home/fuzz/vim-master/src/ex_docmd.c:2567:2
    #17 0x7e49a5 in do_cmdline /home/fuzz/vim-master/src/ex_docmd.c:992:17
    #18 0x7e95f1 in do_cmdline_cmd /home/fuzz/vim-master/src/ex_docmd.c:586:12
    #19 0x144d0a2 in exe_commands /home/fuzz/vim-master/src/main.c:3108:2
    #20 0x144922d in vim_main2 /home/fuzz/vim-master/src/main.c:780:2
    #21 0x143e484 in main /home/fuzz/vim-master/src/main.c:432:12
    #22 0x7f2c12cf60b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/
    #23 0x41fe5d in _start (/home/fuzz/vim-master/src/vim+0x41fe5d)

0x60b00000087f is located 1 bytes to the left of 100-byte region [0x
allocated by thread T0 here:
    #0 0x49b0bd in malloc (/home/fuzz/vim-master/src/vim+0x49b0bd)
    #1 0x4cc79a in lalloc /home/fuzz/vim-master/src/alloc.c:246:11
```

```
    #2 0x4cc67a in alloc /home/fuzz/vim-master/src/alloc.c:151:12
    #3 0x876aa5 in alloc_cmdbuff /home/fuzz/vim-master/src/ex_getln.c:3283:22
    #4 0x8807c0 in init_ccline /home/fuzz/vim-master/src/ex_getln.c:1525:5

    #5 0x865080 in getcmdline_int /home/fuzz/vim-master/src/ex_getln.c:1638:9
    #6 0x86483e in getcmdline /home/fuzz/vim-master/src/ex_getln.c:1571:12
    #7 0x872ce6 in getexline /home/fuzz/vim-master/src/ex_getln.c:2853:12
    #8 0x7e3982 in do_cmdline /home/fuzz/vim-master/src/ex_docmd.c:875:46
    #9 0xb70283 in nv_colon /home/fuzz/vim-master/src/normal.c:3191:19
    #10 0xb45243 in normal_cmd /home/fuzz/vim-master/src/normal.c:930:5
    #11 0x82eefe in exec_normal /home/fuzz/vim-master/src/ex_docmd.c:8753:6
    #12 0x82e728 in exec_normal_cmd /home/fuzz/vim-master/src/ex_docmd.c:8716:5
    #13 0x82e2d9 in ex_normal /home/fuzz/vim-master/src/ex_docmd.c:8634:6
    #14 0x7f7a25 in do_one_cmd /home/fuzz/vim-master/src/ex_docmd.c:2567:2
    #15 0x7e49a5 in do_cmdline /home/fuzz/vim-master/src/ex_docmd.c:992:17
    #16 0xe88e0c in do_source_ext /home/fuzz/vim-master/src/scriptfile.c:1674:5
    #17 0xe85866 in do_source /home/fuzz/vim-master/src/scriptfile.c:1801:12
    #18 0xe8519c in cmd_source /home/fuzz/vim-master/src/scriptfile.c:1174:14
    #19 0xe8487e in ex_source /home/fuzz/vim-master/src/scriptfile.c:1200:2
    #20 0x7f7a25 in do_one_cmd /home/fuzz/vim-master/src/ex_docmd.c:2567:2
    #21 0x7e49a5 in do_cmdline /home/fuzz/vim-master/src/ex_docmd.c:992:17
    #22 0x7e95f1 in do_cmdline_cmd /home/fuzz/vim-master/src/ex_docmd.c:586:12
    #23 0x144d0a2 in exe_commands /home/fuzz/vim-master/src/main.c:3108:2
    #24 0x144922d in vim_main2 /home/fuzz/vim-master/src/main.c:780:2
    #25 0x143e484 in main /home/fuzz/vim-master/src/main.c:432:12
    #26 0x7f2c12cf60b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim-master/src/ex_getln.c:1
Shadow bytes around the buggy address:
  0x0c167fff80b0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c167fff80c0: 00 00 00 00 00 fa fa fa fa fa fa fa fa fa 00 00
  0x0c167fff80d0: 00 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa
  0x0c167fff80e0: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c167fff80f0: 00 fa fa fa fa fa fa fa fa fa fa 00 00 00 00 00
=>0x0c167fff8100: 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa fa[fa]
  0x0c167fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 00 04 fa fa fa
  0x0c167fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8150: fa 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
==75948==ABORTING
```

Bram Moolenaar validated this vulnerability 7 months ago

Thank you for making a simple POC, now I could easily reproduce and use this POC for a regression test.

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 **ef02f1** 7 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Bram Moolenaar 7 months ago Maintainer

Fixed in patch 8.2.4899