Heap-based Buffer Overflow in vim/vim

Valid Reported on Jan 18th 2022

0

Description

Heap-buffer-overflow in vim

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S poc3 -c :qa!
```

POC3 is here.

Bt

```
==728741==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000
READ of size 1 at 0x621000025500 thread T0
    #0 0x8961b1 in utf_head_off /home/zxq/CVE_testing/ASAN-install/vim/src/
    #1 0x989caa in block_insert /home/zxq/CVE_testing/ASAN-install/vim/src/
    #2 0x9891ee in op_insert /home/zxq/CVE_testing/ASAN-install/vim/src/ops
    #3 0x99f0ae in do_pending_operator /home/zxq/CVE_testing/ASAN-install/v
    #4 0x935dfe in normal_cmd /home/zxq/CVE_testing/ASAN-install/vim/src/no
    #5 0x71372b in exec_normal /home/zxq/CVE_testing/ASAN-install/vim/src/e
    #6 0x7132da in exec_normal_cmd /home/zxq/CVE_testing/ASAN-install/vim/s
    #7 0x71300d in ex_normal /home/zxq/CVE_testing/ASAN-install/vim/src/ex_
    #8 0x6ed643 in do_one_cmd /home/zxq/CVE_testing/ASAN-install/vim/src/ex
    #9 0x6e043c in do_cmdline /home/zxq/CVE_testing/ASAN-install/vim/src/ex
    #10 0xb53dd5 in do_source /home/zxq/CVE_testing/ASAN-install/vim/src/so
    #11 0xb513ea in cmd_source /home/zxq/CVE_testing/ASAN-install/vim/src/s
    #12 0xb51140 in ex_source /home/zxq/CVE_testing/ASAN-install/vim/src/so
    #13 0x6ed643 in do_one_cmd /home/zxq/CVE_testing/ASAN-install/vim/src/
    #14 0x6e043c in do_cmdline /home/zxq/CVE_testing/ASAN-i
    #15 0x6e3a53 in do_cmdline_cmd /home/zxq/CVE_testing/ASAN-install/vim/s
```

```
    #16 0xf6bf78 in exe_commands /home/zxq/CVE_testing/ASAN-install/vim/src
    #17 0xf690cd in vim_main2 /home/zxq/CVE_testing/ASAN-install/vim/src/ma
    #18 0xf61baf in main /home/zxq/CVE_testing/ASAN-install/vim/src/main.c:

    #19 0x7f6f765e20b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #20 0x41ee8d in _start (/home/zxq/CVE_testing/ASAN-install/vim/src/vim+

0x621000025500 is located 0 bytes to the right of 4096-byte region [0x62100
allocated by thread T0 here:
    #0 0x4975cd in malloc (/home/zxq/CVE_testing/ASAN-install/vim/src/vim+0
    #1 0x4c70fd in lalloc /home/zxq/CVE_testing/ASAN-install/vim/src/alloc.
    #2 0x4c7049 in alloc /home/zxq/CVE_testing/ASAN-install/vim/src/alloc.c
    #3 0xf72e94 in mf_alloc_bhdr /home/zxq/CVE_testing/ASAN-install/vim/src
    #4 0xf721fe in mf_new /home/zxq/CVE_testing/ASAN-install/vim/src/memfil
    #5 0x8a77e3 in ml_new_data /home/zxq/CVE_testing/ASAN-install/vim/src/m
    #6 0x8c1b04 in ml_append_int /home/zxq/CVE_testing/ASAN-install/vim/src
    #7 0x8b9e09 in ml_append_flush /home/zxq/CVE_testing/ASAN-install/vim/s
    #8 0x8b9cc6 in ml_append_flags /home/zxq/CVE_testing/ASAN-install/vim/s
    #9 0x8b66c7 in ml_append /home/zxq/CVE_testing/ASAN-install/vim/src/mem
    #10 0x7660d8 in readfile /home/zxq/CVE_testing/ASAN-install/vim/src/fil
    #11 0x71ea46 in ex_read /home/zxq/CVE_testing/ASAN-install/vim/src/ex_c
    #12 0x6ed643 in do_one_cmd /home/zxq/CVE_testing/ASAN-install/vim/src/e
    #13 0x6e043c in do_cmdline /home/zxq/CVE_testing/ASAN-install/vim/src/e
    #14 0xb53dd5 in do_source /home/zxq/CVE_testing/ASAN-install/vim/src/so
    #15 0xb513ea in cmd_source /home/zxq/CVE_testing/ASAN-install/vim/src/s
    #16 0xb51140 in ex_source /home/zxq/CVE_testing/ASAN-install/vim/src/so
    #17 0x6ed643 in do_one_cmd /home/zxq/CVE_testing/ASAN-install/vim/src/e
    #18 0x6e043c in do_cmdline /home/zxq/CVE_testing/ASAN-install/vim/src/e
    #19 0x6e3a53 in do_cmdline_cmd /home/zxq/CVE_testing/ASAN-install/vim/s
    #20 0xf6bf78 in exe_commands /home/zxq/CVE_testing/ASAN-install/vim/src
    #21 0xf690cd in vim_main2 /home/zxq/CVE_testing/ASAN-install/vim/src/ma
    #22 0xf61baf in main /home/zxq/CVE_testing/ASAN-install/vim/src/main.c:
    #23 0x7f6f765e20b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/zxq/CVE_testing/ASAN-
Shadow bytes around the buggy address:
  0x0c427fffca50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffca60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffca70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffca80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffca90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
=>0x0c427fffcaa0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffcab0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffcac0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

  0x0c427fffcad0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffcae0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffcaf0: 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
==728741==ABORTING
```

CVE
CVE-2022-0318
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (6.6)

Visibility
Public

Status
Fixed

Found by

zfeixq
@zfeixq
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,631 times.

We are processing your report and will contact the **vim** team within 24 hours. 10 months ago

zfeixq modified the report 10 months ago

We have contacted a member of the **vim** team and are waiting to hear back 10 months ago

Bram Moolenaar 10 months ago Maintainer

The POC is much too long. Please reduce it to the minimal necessary to reproduce the problem.

zfeixq 10 months ago Researcher

Newpoc is here.

Bram Moolenaar 10 months ago Maintainer

I can reproduce it now. The POC is still long and a bit obscure, especially bec
I'll see if I can come up with a simpler test.

Bram Moolenaar validated this vulnerability 10 months ago

zfeixq has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

zfeixq 10 months ago Researcher

Thank you.

Bram Moolenaar 10 months ago Maintainer

Fixed with patch 8.2.4151. The test didn't trigger a valgrind error, could not make it cover the actual problem.

Bram Moolenaar marked this as fixed in 8.2 with commit 57df9e 10 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us