huntr

Buffer Over-read in function grab_file_name in vim/vim

0

✓ Valid Reported on May 13th 2022

Description

Buffer Over-read in function grab_file_name at findfile.c:1947

vim version

```
git log
commit 31ad32a325cc31f0f2bdd530c68bfb856a2187c5 (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_
=================================================================
==1910783==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 1 at 0x602000007092 thread T0
    #0 0x8f43e4 in grab_file_name /home/fuzz/vim/vim/src/findfile.c:1947:2
    #1 0xb97703 in nv_gotofile /home/fuzz/vim/vim/src/normal.c:4061:11
    #2 0xb81feb in nv_g_cmd /home/fuzz/vim/vim/src/normal.c:6066:2
    #3 0xb484d1 in normal_cmd /home/fuzz/vim/vim/src/normal.c:930:5
    #4 0x83001e in exec_normal /home/fuzz/vim/vim/src/ex_docmd.c:8757:6
    #5 0x82f848 in exec_normal_cmd /home/fuzz/vim/vim/src/ex_docmd.c:8720:
    #6 0x82f3f9 in ex_normal /home/fuzz/vim/vim/src/ex_docmd.c:8638:6
    #7 0x7f88a5 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #8 0x7e5825 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #9 0xe8c39c in do_source_ext /home/fuzz/vim/vim/src/scriptfile.c:1674:
    #10 0xe88df6 in do_source /home/fuzz/vim/vim/src/scriptfile.c:1801:12
    #11 0xe8872c in cmd_source /home/fuzz/vim/vim/src/scrip
    #12 0xe87e0e in ex_source /home/fuzz/vim/vim/src/scriptfile.c:1200:2
    #13 0x7f88a5 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #13 0x7f88a5 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #14 0x7e5825 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #15 0x7ea471 in do_cmdline_cmd /home/fuzz/vim/vim/src/ex_docmd.c:586:12
    #16 0x14551a2 in exe_commands /home/fuzz/vim/vim/src/main.c:3108:2
    #17 0x145132d in vim_main2 /home/fuzz/vim/vim/src/main.c:780:2
    #18 0x1446584 in main /home/fuzz/vim/vim/src/main.c:432:12
    #19 0x7ffff7820082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #20 0x41fe5d in _start (/home/fuzz/fuzz-vim/vim/src/vim+0x41fe5d)

0x602000007092 is located 0 bytes to the right of 2-byte region [0x60200000
allocated by thread T0 here:
    #0 0x49b0bd in malloc (/home/fuzz/fuzz-vim/vim/src/vim+0x49b0bd)
    #1 0x4cc79a in lalloc /home/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cc67a in alloc /home/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x54a91d in ins_char_bytes /home/fuzz/vim/vim/src/change.c:1092:12
    #4 0x54b3eb in ins_char /home/fuzz/vim/vim/src/change.c:1007:5
    #5 0x6b3f6f in insertchar /home/fuzz/vim/vim/src/edit.c:2297:6
    #6 0x6ac009 in insert_special /home/fuzz/vim/vim/src/edit.c:2056:2
    #7 0x6917fd in edit /home/fuzz/vim/vim/src/edit.c:1375:3
    #8 0xb9301c in invoke_edit /home/fuzz/vim/vim/src/normal.c:7021:9
    #9 0xb761e5 in nv_edit /home/fuzz/vim/vim/src/normal.c:6991:2
    #10 0xb484d1 in normal_cmd /home/fuzz/vim/vim/src/normal.c:930:5
    #11 0x83001e in exec_normal /home/fuzz/vim/vim/src/ex_docmd.c:8757:6
    #12 0x82f848 in exec_normal_cmd /home/fuzz/vim/vim/src/ex_docmd.c:8720:
    #13 0x82f3f9 in ex_normal /home/fuzz/vim/vim/src/ex_docmd.c:8638:6
    #14 0x7f88a5 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #15 0x7e5825 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #16 0xe8c39c in do_source_ext /home/fuzz/vim/vim/src/scriptfile.c:1674:
    #17 0xe88df6 in do_source /home/fuzz/vim/vim/src/scriptfile.c:1801:12
    #18 0xe8872c in cmd_source /home/fuzz/vim/vim/src/scriptfile.c:1174:14
    #19 0xe87e0e in ex_source /home/fuzz/vim/vim/src/scriptfile.c:1200:2
    #20 0x7f88a5 in do_one_cmd /home/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #21 0x7e5825 in do_cmdline /home/fuzz/vim/vim/src/ex_docmd.c:992:17
    #22 0x7ea471 in do_cmdline_cmd /home/fuzz/vim/vim/src/ex_docmd.c:586:12
    #23 0x14551a2 in exe_commands /home/fuzz/vim/vim/src/main.c:3108:2
    #24 0x145132d in vim_main2 /home/fuzz/vim/vim/src/main.c:780:2
    #25 0x1446584 in main /home/fuzz/vim/vim/src/main.c:432:12
    #26 0x7ffff7820082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/
Shadow bytes around the buggy address:
  0x0c047fff8dc0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8dd0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8de0: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd

  0x0c047fff8df0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8e00: fa fa fd fa fa fa 01 fa fa fa 00 00 fa fa 01 fa
=>0x0c047fff8e10: fa fa[02]fa fa fa 05 fa fa fa fd fa fa fa 01 fa
  0x0c047fff8e20: fa fa fd fa fa fa 02 fa fa fa fa fa fa fa fa fa
  0x0c047fff8e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e60: 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
==1910783==ABORTING
```

poc_h5_s.dat

Impact

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

CVE

CVE-2022-1720
(Published)

Vulnerability Type
CWE-126: Buffer Over-read

Severity
Medium (6.6)

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 1,155 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 validated this vulnerability 6 months ago

Chat with us

I can see that it is reading just after the NUL that terminates the line.

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 6 months ago Maintainer

Fixed with Patch 8.2.4956

Bram Moolenaar marked this as fixed in **8.2** with commit **395bd1** 6 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

terms

privacy policy