Heap Use After Free in function ex_diffgetput in vim/vim

0

✓ Valid Reported on Jun 29th 2022

Description

Heap Use After Free in function ex_diffgetput at diff.c:2790

vim version

```
git log
commit 75417d960bd17a5b701cfb625b8864dacaf0cc39 (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_huaf3_s.dat -c :qa

=================================================================
==683647==ERROR: AddressSanitizer: heap-use-after-free on address 0x60d0000
READ of size 8 at 0x60d000009018 thread T0
    #0 0x5fb91e in ex_diffgetput /home/fuzz/fuzz/vim/afl/src/diff.c:2790:6
    #1 0x5f9af2 in nv_diffgetput /home/fuzz/fuzz/vim/afl/src/diff.c:2642:5
    #2 0xb6c9ac in nv_put_opt /home/fuzz/fuzz/vim/afl/src/normal.c:7262:6
    #3 0xb52d27 in nv_put /home/fuzz/fuzz/vim/afl/src/normal.c:7237:5
    #4 0xb1fe8f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #5 0x81539e in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812:
    #6 0x814bc8 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8
    #7 0x814779 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:6
    #8 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #9 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/e
    #10 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #11 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #11 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:180
    #12 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #13 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:120
    #14 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #15 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #16 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #17 0x1424092 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #18 0x142022b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #19 0x141573d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #20 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #21 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x60d000009018 is located 8 bytes inside of 136-byte region [0x60d00000901
freed by thread T0 here:
    #0 0x499a52 in free (/home/fuzz/fuzz/vim/afl/src/vim+0x499a52)
    #1 0x4cbdf6 in vim_free /home/fuzz/fuzz/vim/afl/src/alloc.c:624:2
    #2 0x5eae9f in diff_mark_adjust_tp /home/fuzz/fuzz/vim/afl/src/diff.c:5
    #3 0x5e8d09 in diff_mark_adjust /home/fuzz/fuzz/vim/afl/src/diff.c:279
    #4 0xa28dd2 in mark_adjust_internal /home/fuzz/fuzz/vim/afl/src/mark.c
    #5 0xa23ce8 in mark_adjust /home/fuzz/fuzz/vim/afl/src/mark.c:1004:5
    #6 0x5fce79 in ex_diffgetput /home/fuzz/fuzz/vim/afl/src/diff.c:2905:3
    #7 0x5f9af2 in nv_diffgetput /home/fuzz/fuzz/vim/afl/src/diff.c:2642:5
    #8 0xb6c9ac in nv_put_opt /home/fuzz/fuzz/vim/afl/src/normal.c:7262:6
    #9 0xb52d27 in nv_put /home/fuzz/fuzz/vim/afl/src/normal.c:7237:5
    #10 0xb1fe8f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #11 0x81539e in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812
    #12 0x814bc8 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c
    #13 0x814779 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:6
    #14 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #15 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #16 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c
    #17 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #18 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #19 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #20 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #21 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #22 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #23 0x1424092 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #24 0x142022b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #25 0x141573d in main /home/fuzz/fuzz/vim/afl/src/main.
    #26 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
```

```
previously 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 0x600782 in diff_alloc_new /home/fuzz/fuzz/vim/afl/src/diff.c:558:12
    #4 0x605c2b in diff_read /home/fuzz/fuzz/vim/afl/src/diff.c:1829:11
    #5 0x5ef64e in diff_try_update /home/fuzz/fuzz/vim/afl/src/diff.c:905:2
    #6 0x5ee4d9 in ex_diffupdate /home/fuzz/fuzz/vim/afl/src/diff.c:991:5
    #7 0x5ff67a in diff_lnum_win /home/fuzz/fuzz/vim/afl/src/diff.c:3158:2
    #8 0x545e5a in changed_bytes /home/fuzz/fuzz/vim/afl/src/change.c:728:1
    #9 0x54d67e in ins_char_bytes /home/fuzz/fuzz/vim/afl/src/change.c:1125
    #10 0x54e0ab in ins_char /home/fuzz/fuzz/vim/afl/src/change.c:1014:5
    #11 0x6979df in insertchar /home/fuzz/fuzz/vim/afl/src/edit.c:2275:6
    #12 0x68fa79 in insert_special /home/fuzz/fuzz/vim/afl/src/edit.c:2038:
    #13 0x675137 in edit /home/fuzz/fuzz/vim/afl/src/edit.c:1359:3
    #14 0xb6a9cc in invoke_edit /home/fuzz/fuzz/vim/afl/src/normal.c:7035:9
    #15 0xb6c6e4 in n_opencmd /home/fuzz/fuzz/vim/afl/src/normal.c:6279:6
    #16 0xb52cc6 in nv_open /home/fuzz/fuzz/vim/afl/src/normal.c:7416:2
    #17 0xb1fe8f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #18 0x81539e in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812
    #19 0x814bc8 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:
    #20 0x814779 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:6
    #21 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #22 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #23 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #24 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #25 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #26 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #27 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #28 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #29 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/fuzz/vim/afl/src/
Shadow bytes around the buggy address:
  0x0c1a7fff91b0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1a7fff91c0: fd fd fd fd fd fd fa fa fa fa fa fa fa fa fd fd
  0x0c1a7fff91d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1a7fff91e0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00
  0x0c1a7fff91f0: 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa
=>0x0c1a7fff9200: fa fa fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd
```

```
=>0x0c1a7fff9200: fa fa fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1a7fff9210: fd fd fd fa fa fa fa fa fa fa fa fa fd fd fd fd
  0x0c1a7fff9220: fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa

  0x0c1a7fff9230: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9250: 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
==683647==ABORTING
```

poc_huaf3_s.dat

Impact

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

CVE

CVE-2022-2289

(Published)

(Published)

Vulnerability Type
CWE-416: Use After Free

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 754 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 back 5 months ago

Bram Moolenaar validated this vulnerability 5 months ago

I can reproduce it. The POC is too complicated to use as a test. Can you do it without the mapping of "0"?

Chat with us

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 9.0.0026

Bram Moolenaar marked this as fixed in **9.0** with commit **c5274d** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us