Out-of-bounds write in function vim_regsub_both in vim/vim

0

Valid Reported on May 16th 2022

Description

Out-of-bounds write in function vim_regsub_both at regexp.c:1954

vim version

```
git log
commit 5a8fad32ea9c075f045b37d6c7739891d458f82b (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_
==================================================================
==19509==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000
WRITE of size 2 at 0x606000003175 thread T0
    #0 0x485357 in strcpy (/home/fuzz/fuzz/vim/vim/src/vim+0x485357)
    #1 0xce59a4 in vim_regsub_both /home/fuzz/fuzz/vim/vim/src/regexp.c:195
    #2 0xce9da3 in vim_regsub_multi /home/fuzz/fuzz/vim/vim/src/regexp.c:18
    #3 0x7ae5ad in ex_substitute /home/fuzz/fuzz/vim/vim/src/ex_cmds.c:4521
    #4 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #5 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #6 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1
    #7 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:
    #8 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174
    #9 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scr
    #10 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/
    #11 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
```

```
    #12 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #13 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
    #14 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2

    #15 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #16 0x7f9372ae2082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #17 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x606000003175 is located 0 bytes to the right of 53-byte region [0x6060000
allocated by thread T0 here:
    #0 0x499ccd in malloc (/home/fuzz/fuzz/vim/vim/src/vim+0x499ccd)
    #1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x7ae273 in ex_substitute /home/fuzz/fuzz/vim/vim/src/ex_cmds.c:4486
    #4 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #5 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #6 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1
    #7 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:
    #8 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174
    #9 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200:
    #10 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
    #11 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #12 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #13 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
    #14 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #15 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #16 0x7f9372ae2082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz/vim/vim/sr
Shadow bytes around the buggy address:
  0x0c0c7fff85d0: fa fa fa fa fd fd fd fd fd fd fd fa fa fa fa fa
  0x0c0c7fff85e0: fd fd fd fd fd fd fd fd fa fa fa fa 00 00 00 00
  0x0c0c7fff85f0: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0c7fff8600: fa fa fa fa 00 00 00 00 00 00 00 fa fa fa fa fa
  0x0c0c7fff8610: 00 00 00 00 00 00 00 fa fa fa fa fa 00 00 00 00
=>0x0c0c7fff8620: 00 00 00 fa fa fa fa fa 00 00 00 00 00 00[05]fa
  0x0c0c7fff8630: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8640: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8650: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8660: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8670: 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
==19509==ABORTING
```

poc_obw_s.dat

Impact

This may result in corruption of sensitive information, a crash, or code execution among other things.

CVE
CVE-2022-1785
(Published)

Vulnerability Type
CWE-787: Out-of-bounds Write

Severity
High (7.3)

Registry
Other

Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 989 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

I can reproduce the problem. The POC can be slightly simplified by changing the special character by two zeroes.

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

Fixed in patch 8.2.4977

Bram Moolenaar marked this as fixed in **8.2** with commit **e2bd86** 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation