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

0

Valid Reported on Jun 16th 2022

Description

Out-of-bounds write in function vim_regsub_both at regexp.c:1973

vim version

```
git log
commit 83497f875881973df772cc4cc593766345df6c4a (HEAD -> master, tag: v8.2.
```

POC

```
root@fuzz-vm0-187:/home/fuzz/fuzz/vim/afl/src# ./vim -u NONE -i NONE -n -m
================================================================
==25109==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000
WRITE of size 2 at 0x606000000f55 thread T0
    #0 0x485337 in strcpy (/home/fuzz/fuzz/vim/afl/src/vim+0x485337)
    #1 0xcebc36 in vim_regsub_both /home/fuzz/fuzz/vim/afl/src/regexp.c:197
    #2 0xcf06eb in vim_regsub_multi /home/fuzz/fuzz/vim/afl/src/regexp.c:19
    #3 0x7b4328 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:4531
    #4 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #5 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:17
    #6 0xe58b5e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1
    #7 0xe555f6 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801:
    #8 0xe54f33 in cmd_source /home/fuzz/fuzz/vim/afl/src/sc
    #9 0xe5463e in ex_source /home/fuzz/fuzz/vim/afl/src/sc
    #10 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
```

```
    #11 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #12 0x7ced81 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #13 0x1422702 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2

    #14 0x141e89b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #15 0x1413dad in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #16 0x7fc0b29a6082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #17 0x41ea4d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea4d)

0x606000000f55 is located 0 bytes to the right of 53-byte region [0x6060000
allocated by thread T0 here:
    #0 0x499cad in malloc (/home/fuzz/fuzz/vim/afl/src/vim+0x499cad)
    #1 0x4cb382 in lalloc /home/fuzz/fuzz/vim/afl/src/alloc.c:246:11
    #2 0x4cb26a in alloc /home/fuzz/fuzz/vim/afl/src/alloc.c:151:12
    #3 0x7b3f23 in ex_substitute /home/fuzz/fuzz/vim/afl/src/ex_cmds.c:449
    #4 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #5 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:17
    #6 0xe58b5e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1
    #7 0xe555f6 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801:
    #8 0xe54f33 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1174
    #9 0xe5463e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200:
    #10 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #11 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #12 0x7ced81 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #13 0x1422702 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #14 0x141e89b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #15 0x1413dad in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #16 0x7fc0b29a6082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz/vim/afl/sr
Shadow bytes around the buggy address:
  0x0c0c7fff8190: fd fd fd fd fd fd fd fa fa fa fa fa 00 00 00 00
  0x0c0c7fff81a0: 00 00 05 fa fa fa fa fa fd fd fd fd fd fd fd fa
  0x0c0c7fff81b0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c7fff81c0: 00 00 00 00 00 00 00 fa fa fa fa fa 00 00 00 00
  0x0c0c7fff81d0: 00 00 00 fa fa fa fa fa 00 00 00 00 00 00 00 fa
=>0x0c0c7fff81e0: fa fa fa fa 00 00 00 00 00 00[05]fa fa fa fa fa
  0x0c0c7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c0c7fff8230: 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
==25109==ABORTING
```

poc_obw7_s.dat

Impact

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

CVE
CVE-2022-2129
(Published)

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

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 793 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 the problem. Also with a further simplified POC.

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 8.2.5126, which includes a regression test.

Bram Moolenaar marked this as fixed in 8.2 with commit d6211a 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

ren0216 5 months ago

Found that patch 8.2.4616 can not reproduce the problem, but patch 8.2.4617 can not , thus , dose this mean 4617 taking the vulnerability in ?

Bram Moolenaar 5 months ago Maintainer

Not sure. Sometimes a patch does not fix an issue, but changes the way it is reproduced. Especially issues that rely on text being in a certain allocated area. I made patch 9.0.0013 specifically to make it simpler to reproduce issues.

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team