huntr

Heap-based Buffer Overflow in function vim_regsub_both in vim/vim

0

✓ Valid Reported on May 25th 2022

Description

Heap-based Buffer Overflow in function vim_regsub_both at regexp.c:1954

vim version

```
git log
commit 4d97a565ae8be0d4debba04ebd2ac3e75a0c8010 (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_
=================================================================
==2583207==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60600
WRITE of size 2 at 0x606000003595 thread T0
    #0 0x485357 in strcpy (/home/fuzz/fuzz/vim/vim/src/vim+0x485357)
    #1 0xced574 in vim_regsub_both /home/fuzz/fuzz/vim/vim/src/regexp.c:195
    #2 0xcf1973 in vim_regsub_multi /home/fuzz/fuzz/vim/vim/src/regexp.c:18
    #3 0x7b4663 in ex_substitute /home/fuzz/fuzz/vim/vim/src/ex_cmds.c:452
    #4 0x7dd699 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #5 0x7ca405 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #6 0xe5998c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1
    #7 0xe563e6 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:
    #8 0xe55d1c in cmd_source /home/fuzz/fuzz/vim/vim/src/sc
    #9 0xe553fe in ex_source /home/fuzz/fuzz/vim/vim/src/sc
    #10 0x7dd699 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
```

Chat with us

```
    #11 0x7ca405 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #12 0x7cf0a1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #13 0x14258e2 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2

    #14 0x1421a7b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #15 0x1417175 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #16 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #17 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x606000003595 is located 0 bytes to the right of 53-byte region [0x606000
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 0x7b42c7 in ex_substitute /home/fuzz/fuzz/vim/vim/src/ex_cmds.c:4491
    #4 0x7dd699 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:2
    #5 0x7ca405 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #6 0xe5998c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1
    #7 0xe563e6 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:
    #8 0xe55d1c in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174
    #9 0xe553fe in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200:
    #10 0x7dd699 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2568:
    #11 0x7ca405 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #12 0x7cf0a1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #13 0x14258e2 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #14 0x1421a7b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #15 0x1417175 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #16 0x7ffff7bec082 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:
  0x0c0c7fff8660: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c7fff8670: fd fd fd fd fd fd fd fd fa fa fa fa 00 00 00 00
  0x0c0c7fff8680: 00 00 02 fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c7fff8690: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c7fff86a0: 00 00 00 00 00 00 02 fa fa fa fa fa 00 00 00 00
=>0x0c0c7fff86b0: 00 00[05]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff86c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff86d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff86e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff86f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8700: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8700: 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
==2583207==ABORTING
```

poc_obw5_s.dat

Impact

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

CVE
CVE-2022-1942
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

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 1,048 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 6 months ago Maintainer

I cannot reproduce this problem. Please sync to head, it might have already been fixed by Patch 8.2.5007

Bram Moolenaar 6 months ago Maintainer

Hmm, your comment "tag: v8.2.5014" indicates that patch 8.2.5007 would already be included Nevertheless, I cannot reproduce.

Chat with us

TDHX ICS Security modified the report 6 months ago

TDHX 6 months ago

Researcher

Found another Heap-based Buffer Overflow at regexp.c:1954 after sync to head(tag: v8.2.5037).
Wish you could reproduce this one.
Report is modified accordingly

We have sent a follow up to the **vim** team. We will try again in 7 days. 6 months ago

Bram Moolenaar 6 months ago

Maintainer

Yes, this one I can reproduce. The POC can be simplified a bit more and I'll use that for a test.

Bram Moolenaar validated this vulnerability 6 months ago

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 8.2.5043

Bram Moolenaar marked this as fixed in **8.2** with commit **71223e** 6 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