Heap-based Buffer Overflow in function ins_compl_infercase_gettext() in vim/vim

0

Valid Reported on Jul 15th 2022

Description

Heap-based Buffer Overflow in function ins_compl_infercase_gettext at src/insexpand.c:645

vim version

```
commit 3a393790a4fd7a5edcafbb55cd79438b6e641714
Author: Dominique Pelle <dominique.pelle@gmail.com>
Date:   Thu Jul 14 17:40:49 2022 +0100

    patch 9.0.0053: E1281 not tested with the old regexp engine

    Problem:    E1281 not tested with the old regexp engine.
    Solution:   Loop over the values of 'regexp'. (Dominique Pellé, closes
```

To reproduce

```
export CFLAGS="-g3 -fsanitize=address -fno-common -fno-omit-frame-pointer -
export LDFLAGS="-g3 -fsanitize=address -fno-common -fno-omit-frame-pointer
./configure
make -j4
./src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_hbor4_s.dat -c :qa!
```

Stack information

```
=================================================================
==33751==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000(
READ of size 1026 at 0x619000000981 thread T0
    #0 0x7fa2ab4b7fe3  (/usr/lib64/libasan.so.6+0x52fe3)
    #1 0x66cbdb in ins_compl_infercase_gettext /root/github_vim/src/insexpa
    #2 0x66d350 in ins_compl_add_infercase /root/github_vim/src/insexpand.c
    #3 0x6796d9 in get_next_default_completion /root/github_vim/src/insexpa
    #4 0x6799db in get_next_completion_match /root/github_vim/src/insexpanc
    #5 0x679e91 in ins_compl_get_exp /root/github_vim/src/insexpand.c:3806
    #6 0x67aafa in find_next_completion_match /root/github_vim/src/insexpar
    #7 0x67ae9e in ins_compl_next /root/github_vim/src/insexpand.c:4142
    #8 0x67e01c in ins_complete /root/github_vim/src/insexpand.c:4993
    #9 0x4d8fb4 in edit /root/github_vim/src/edit.c:1281
    #10 0x75c69a in op_change /root/github_vim/src/ops.c:1758
    #11 0x76e7ed in do_pending_operator /root/github_vim/src/ops.c:4041
    #12 0x724e12 in normal_cmd /root/github_vim/src/normal.c:961
    #13 0x5a98ab in exec_normal /root/github_vim/src/ex_docmd.c:8814
    #14 0x5a9674 in exec_normal_cmd /root/github_vim/src/ex_docmd.c:8777
    #15 0x5a8f0b in ex_normal /root/github_vim/src/ex_docmd.c:8695
    #16 0x5857c0 in do_one_cmd /root/github_vim/src/ex_docmd.c:2570
    #17 0x57c853 in do_cmdline /root/github_vim/src/ex_docmd.c:992
    #18 0x89e715 in do_source_ext /root/github_vim/src/scriptfile.c:1674
    #19 0x89f8aa in do_source /root/github_vim/src/scriptfile.c:1801
    #20 0x89c32d in cmd_source /root/github_vim/src/scriptfile.c:1174
    #21 0x89c3a0 in ex_source /root/github_vim/src/scriptfile.c:1200
    #22 0x5857c0 in do_one_cmd /root/github_vim/src/ex_docmd.c:2570
    #23 0x57c853 in do_cmdline /root/github_vim/src/ex_docmd.c:992
    #24 0x57ab0e in do_cmdline_cmd /root/github_vim/src/ex_docmd.c:586
    #25 0xb6de7a in exe_commands /root/github_vim/src/main.c:3133
    #26 0xb66d6a in vim_main2 /root/github_vim/src/main.c:780
    #27 0xb66570 in main /root/github_vim/src/main.c:432
    #28 0x7fa2ab18220f in __libc_start_call_main ../sysdeps/nptl/libc_start
    #29 0x7fa2ab1822bb in __libc_start_main_impl ../csu/libc-start.c:409
    #30 0x404f24 in _start (/root/github_vim/src/vim+0x404f24)

0x619000000981 is located 0 bytes to the right of 1025-byte region [0x61900
allocated by thread T0 here:
    #0 0x7fa2ab5141c7 in __interceptor_malloc (/usr/lib64/li
    #1 0x405370 in lalloc /root/github_vim/src/alloc.c:246
    #2 0x405161 in alloc /root/github_vim/src/alloc.c:151
```

```
    #3 0xb66fc1 in common_init /root/github_vim/src/main.c:914
    #4 0xb66220 in main /root/github_vim/src/main.c:185
    #5 0x7fa2ab18220f in __libc_start_call_main ../sysdeps/nptl/libc_start_


SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib64/libasan.so.6+0x
Shadow bytes around the buggy address:
  0x0c327fff80e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff80f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8130:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8150: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8160: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8170: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8180: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==33751==ABORTING
```

POC

https://raw.githubusercontent.com/JieyongMa/poc/main/vim/poc_hbor4_s.dat

Impact

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

CVE
CVE-2022-2522
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.8)

Registry
Other

Affected Version
vim-9.0.0053

Visibility
Public

Status
Fixed

Found by

xiaoge1001
@xiaoge1001
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 905 times.

We are processing your report and will contact the **vim** team within 24 hours. 4 months ago

xiaoge1001 modified the report 4 months ago

We have contacted a member of the **vim** team and are waiting to hear back 4 months ago

We have sent a follow up to the **vim** team. We will try again in 7 days. 4 months ago

xiaoge1001 4 months ago Researcher

There was no response for a long time, so I decided to try to fix it.

xiaoge1001 submitted a patch 4 months ago

xiaoge1001 4 months ago Researcher

I have verified that the patch is valid and the problem will not reproduce.

A **vim/vim** maintainer validated this vulnerability 4 months ago

The POC is rather complicated, Ken Takata found a much simpler one.

xiaoge1001 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **vim/vim** maintainer 4 months ago

I would like to mark this as fixed by patch 9.0.0060, but I can't select myself as fixer. The patch suggested above is not a good fix.
@admin

Jamie Slome 4 months ago Admin

Hi Bram, just responded to your e-mail. But in short, you need to ensure that you are not auth'ed as a magic maintainer, but instead are signed in with your GitHub account.

Please clear any tokens from your URL, and sign out / sign in again. Should work 👍

Bram Moolenaar marked this as fixed in **9.0.0060** with commit **5fa9f2** 4 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

xiaoge1001 4 months ago Researcher

@brammool There is a problem with the associated patch. It should be patch 9.0.0060 not patch 9.0.0061, but the link given above is the link of patch 9.0.0061(https://www.github.com/vim/vim/commit/5fa9f2).
The patch given by NVD is also patch 9.0.0061, which should be problematic.

Jamie Slome 4 months ago Admin

@Bram - let me know if you need any support on the above, i.e. adjusting the CVE 👍

Bram Moolenaar 4 months ago

I guess the right commit is b9e717367c395490149495cf375911b5d9de889e

Note that I never use those hex numbers, we use human-readable patch numbers.

Jamie Slome 4 months ago Admin

@bram - would you like me to update the report and CVE?

Bram Moolenaar 4 months ago

Whatever. I only care about fixing problems, I don't care much about the boo

Sign in to join this conversation

Chat with us