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

0

Valid Reported on Jul 6th 2022

Description

Heap-based Buffer Overflow in function ins_compl_add at insexpand.c:751

vim version

```
git log
commit 324478037923feef1eb8a771648e38ade9e5e05a (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_hbor4_s.dat -c :qa
==================================================================
==3114==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61e00008
READ of size 1 at 0x61e0000827cb thread T0
    #0 0x9b3130 in ins_compl_add /home/fuzz/fuzz/vim/afl/src/insexpand.c:75
    #1 0x9b1294 in ins_compl_add_infercase /home/fuzz/fuzz/vim/afl/src/inse
    #2 0x9d137b in get_next_default_completion /home/fuzz/fuzz/vim/afl/src/
    #3 0x9cc7f7 in get_next_completion_match /home/fuzz/fuzz/vim/afl/src/in
    #4 0x9c9a7e in ins_compl_get_exp /home/fuzz/fuzz/vim/afl/src/insexpand.
    #5 0x9c8438 in find_next_completion_match /home/fuzz/fuzz/vim/afl/src/i
    #6 0x9c0f04 in ins_compl_next /home/fuzz/fuzz/vim/afl/src/insexpand.c:4
    #7 0x9c197c in ins_complete /home/fuzz/fuzz/vim/afl/src/insexpand.c:495
    #8 0x674939 in edit /home/fuzz/fuzz/vim/afl/src/edit.c:1
    #9 0xb989c7 in op_change /home/fuzz/fuzz/vim/afl/src/op
    #10 0xbb25f7 in do_pending_operator /home/fuzz/fuzz/vim/afl/src/ops.c:4
```

```
    #11 0xb21ac3 in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:961:2
    #12 0x8156fe in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8814
    #13 0x814f28 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:

    #14 0x814ad9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8695:6
    #15 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #16 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #17 0xe5c8fe in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #18 0xe59396 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #19 0xe58cd3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #20 0xe583de in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #21 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #22 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #23 0x7cf591 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #24 0x1427482 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #25 0x142361b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #26 0x1418b2d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #27 0x7fd83cb66082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #28 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x61e0000827cb is located 125 bytes to the right of 2766-byte region [0x61e
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 0xf90f0d in vim_strnsave /home/fuzz/fuzz/vim/afl/src/strings.c:44:9
    #4 0x9b349a in ins_compl_add /home/fuzz/fuzz/vim/afl/src/insexpand.c:76
    #5 0x9b1294 in ins_compl_add_infercase /home/fuzz/fuzz/vim/afl/src/inse
    #6 0x9d137b in get_next_default_completion /home/fuzz/fuzz/vim/afl/src/
    #7 0x9cc7f7 in get_next_completion_match /home/fuzz/fuzz/vim/afl/src/in
    #8 0x9c9a7e in ins_compl_get_exp /home/fuzz/fuzz/vim/afl/src/insexpand.
    #9 0x9c8438 in find_next_completion_match /home/fuzz/fuzz/vim/afl/src/i
    #10 0x9c0f04 in ins_compl_next /home/fuzz/fuzz/vim/afl/src/insexpand.c:
    #11 0x9c197c in ins_complete /home/fuzz/fuzz/vim/afl/src/insexpand.c:49
    #12 0x674939 in edit /home/fuzz/fuzz/vim/afl/src/edit.c:1281:10
    #13 0xb989c7 in op_change /home/fuzz/fuzz/vim/afl/src/ops.c:1758:14
    #14 0xbb25f7 in do_pending_operator /home/fuzz/fuzz/vim/afl/src/ops.c:4
    #15 0xb21ac3 in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:961:2
    #16 0x8156fe in exec_normal /home/fuzz/fuzz/vim/afl/src/
    #17 0x814f28 in exec_normal_cmd /home/fuzz/fuzz/vim/afl
    #18 0x814ad9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8695:6
```

```
    #19 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #20 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #21 0xe5c8fe in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:

    #22 0xe59396 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #23 0xe58cd3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #24 0xe583de in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1206
    #25 0x7dda59 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #26 0x7ca915 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #27 0x7cf591 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #28 0x1427482 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #29 0x142361b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/afl/src
Shadow bytes around the buggy address:
  0x0c3c800084a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3c800084b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3c800084c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3c800084d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3c800084e0: 00 00 00 00 00 00 00 00 00 06 fa fa fa fa fa fa
=>0x0c3c800084f0: fa fa fa fa fa fa fa fa fa[fa]fa fa fa fa fa fa
  0x0c3c80008500: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c80008510: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c80008520: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c80008530: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c80008540: 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
  ==3114==ABORTING
```

poc_hbor4_s.dat

Impact

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

CVE
CVE-2022-2343
(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 833 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. There must be a much simpler way to reproduc this: using a line more than 1030 bytes long.

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 marked this as fixed in **9.0.0044** with commit **caea66** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

xiaoge1001 4 months ago

After fixing the vulnerability, there are new problems, and the corresponding information is as follows:

```
=================================================================
==33751==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000981 at pc
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/
    #2 0x66d350 in ins_compl_add_infercase /root/github_vim/src/insexpand.c:725
```

```
    #3 0x6796d9 in get_next_default_completion /root/github_vim/src/insexpand.c:3668
    #4 0x6799db in get_next_completion_match /root/github_vim/src/insexpand.c:3733
    #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/insexpand.c:4041

    #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_call_main.
    #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 [0x619000000580,0x6
allocated by thread T0 here:
    #0 0x7fa2ab5141c7 in __interceptor_malloc (/usr/lib64/libasan.so.6+0xaf1c7)
    #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_call_main.h

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib64/libasan.so.6+0x52fe3)
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
  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
```

Occurrences

> Sign in to join this conversation