huntr

Heap-based buffer overflow in function vim_iswordp_buf in vim/vim

0

Valid Reported on Jul 8th 2022

Description

Heap-based buffer overflow in function `vim_iswordp_buf` at charset.c:835

Version

```
commit fee0c4aa99eb0a7a801dade758ce5e04b48c15d1 (HEAD -> master, origin/mas
```

Proof of Concept

```
guest@elk:~/trung$ valgrind ./vim_latest/src/vim  -u NONE -i NONE -n -m -X
==26915== Memcheck, a memory error detector
==26915== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==26915== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright inf
==26915== Command: ./vim_latest/src/vim -u NONE -i NONE -n -m -X -Z -e -s -
==26915==
==26915== Invalid read of size 1
==26915==    at 0x37AB16: vim_iswordp_buf (charset.c:835)
==26915==    by 0x1FCF99: ins_comp_get_next_word_or_line (insexpand.c:3511)
==26915==    by 0x1FCF99: get_next_default_completion (insexpand.c:3663)
==26915==    by 0x1FCF99: get_next_completion_match (insexpand.c:3733)
==26915==    by 0x1FCF99: ins_compl_get_exp (insexpand.c:3806)
==26915==    by 0x1FCF99: find_next_completion_match (insexpand.c:4041)
==26915==    by 0x1FCF99: ins_compl_next (insexpand.c:4142)
==26915==    by 0x1FEB7A: ins_complete (insexpand.c:4993)
==26915==    by 0x180846: edit (edit.c:1281)
==26915==    by 0x22FBF9: invoke_edit.isra.1 (normal.c:7037)
```

Chat with us

```
==26915==    by 0x231E31: n_opencmd (normal.c:6281)
==26915==    by 0x231E31: nv_open (normal.c:7418)
==26915==    by 0x238C14: normal_cmd (normal.c:939)

==26915==    by 0x1B6AFC: exec_normal (ex_docmd.c:8809)
==26915==    by 0x1B6D5F: ex_normal (ex_docmd.c:8695)
==26915==    by 0x1BB67D: do_one_cmd (ex_docmd.c:2570)
==26915==    by 0x1BB67D: do_cmdline (ex_docmd.c:992)
==26915==    by 0x2AC8C0: do_source_ext (scriptfile.c:1674)
==26915==    by 0x2AD8B3: do_source (scriptfile.c:1801)
==26915==    by 0x2AD8B3: cmd_source (scriptfile.c:1174)
==26915==  Address 0x5e5f8d0 is 0 bytes after a block of size 4,096 alloc'd
==26915==    at 0x4C31B0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-
==26915==    by 0x140E20: lalloc (alloc.c:246)
==26915==    by 0x381DCA: mf_alloc_bhdr.isra.3 (memfile.c:884)
==26915==    by 0x382BA6: mf_new (memfile.c:375)
==26915==    by 0x214D7F: ml_new_data (memline.c:4111)
==26915==    by 0x217C3C: ml_open (memline.c:394)
==26915==    by 0x151064: open_buffer (buffer.c:186)
==26915==    by 0x380F49: create_windows (main.c:2902)
==26915==    by 0x380F49: vim_main2 (main.c:711)
==26915==    by 0x13F88C: main (main.c:432)
==26915==
==26915== Invalid read of size 1
==26915==    at 0x1FA1C4: find_word_start (insexpand.c:1626)
==26915==    by 0x1FCFA5: ins_comp_get_next_word_or_line (insexpand.c:3514)
==26915==    by 0x1FCFA5: get_next_default_completion (insexpand.c:3663)
==26915==    by 0x1FCFA5: get_next_completion_match (insexpand.c:3733)
==26915==    by 0x1FCFA5: ins_compl_get_exp (insexpand.c:3806)
==26915==    by 0x1FCFA5: find_next_completion_match (insexpand.c:4041)
==26915==    by 0x1FCFA5: ins_compl_next (insexpand.c:4142)
==26915==    by 0x1FEB7A: ins_complete (insexpand.c:4993)
==26915==    by 0x180846: edit (edit.c:1281)
==26915==    by 0x22FBF9: invoke_edit.isra.1 (normal.c:7037)
==26915==    by 0x231E31: n_opencmd (normal.c:6281)
==26915==    by 0x231E31: nv_open (normal.c:7418)
==26915==    by 0x238C14: normal_cmd (normal.c:939)
==26915==    by 0x1B6AFC: exec_normal (ex_docmd.c:8809)
==26915==    by 0x1B6D5F: ex_normal (ex_docmd.c:8695)
==26915==    by 0x1BB67D: do_one_cmd (ex_docmd.c:2570)
==26915==    by 0x1BB67D: do_cmdline (ex_docmd.c:992)
```

```
==26915==    by 0x2AC8C0: do_source_ext (scriptfile.c:1674)
==26915==    by 0x2AD8B3: do_source (scriptfile.c:1801)
==26915==    by 0x2AD8B3: cmd_source (scriptfile.c:1174)

==26915==  Address 0x5e5f8d0 is 0 bytes after a block of size 4,096 alloc'd
==26915==    at 0x4C31B0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-
==26915==    by 0x140E20: lalloc (alloc.c:246)
==26915==    by 0x381DCA: mf_alloc_bhdr.isra.3 (memfile.c:884)
==26915==    by 0x382BA6: mf_new (memfile.c:375)
==26915==    by 0x214D7F: ml_new_data (memline.c:4111)
==26915==    by 0x217C3C: ml_open (memline.c:394)
==26915==    by 0x151064: open_buffer (buffer.c:186)
==26915==    by 0x380F49: create_windows (main.c:2902)
==26915==    by 0x380F49: vim_main2 (main.c:711)
==26915==    by 0x13F88C: main (main.c:432)
==26915==
==26915== Invalid read of size 1
==26915==    at 0x211BD4: mb_get_class_buf (mbyte.c:843)
==26915==    by 0x1FA28C: find_word_end (insexpand.c:1647)
==26915==    by 0x1FCFAD: ins_comp_get_next_word_or_line (insexpand.c:3517)
==26915==    by 0x1FCFAD: get_next_default_completion (insexpand.c:3663)
==26915==    by 0x1FCFAD: get_next_completion_match (insexpand.c:3733)
==26915==    by 0x1FCFAD: ins_compl_get_exp (insexpand.c:3806)
==26915==    by 0x1FCFAD: find_next_completion_match (insexpand.c:4041)
==26915==    by 0x1FCFAD: ins_compl_next (insexpand.c:4142)
==26915==    by 0x1FEB7A: ins_complete (insexpand.c:4993)
==26915==    by 0x180846: edit (edit.c:1281)
==26915==    by 0x22FBF9: invoke_edit.isra.1 (normal.c:7037)
==26915==    by 0x231E31: n_opencmd (normal.c:6281)
==26915==    by 0x231E31: nv_open (normal.c:7418)
==26915==    by 0x238C14: normal_cmd (normal.c:939)
==26915==    by 0x1B6AFC: exec_normal (ex_docmd.c:8809)
==26915==    by 0x1B6D5F: ex_normal (ex_docmd.c:8695)
==26915==    by 0x1BB67D: do_one_cmd (ex_docmd.c:2570)
==26915==    by 0x1BB67D: do_cmdline (ex_docmd.c:992)
==26915==    by 0x2AC8C0: do_source_ext (scriptfile.c:1674)
==26915==  Address 0x5e5f8d0 is 0 bytes after a block of size 4,096 alloc'd
==26915==    at 0x4C31B0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-
==26915==    by 0x140E20: lalloc (alloc.c:246)
==26915==    by 0x381DCA: mf_alloc_bhdr.isra.3 (memfile.c:8
==26915==    by 0x382BA6: mf_new (memfile.c:375)
```

```
==26915==    by 0x214D7F: ml_new_data (memline.c:4111)
==26915==    by 0x217C3C: ml_open (memline.c:394)
==26915==    by 0x151064: open_buffer (buffer.c:186)

==26915==    by 0x380F49: create_windows (main.c:2902)
==26915==    by 0x380F49: vim_main2 (main.c:711)
==26915==    by 0x13F88C: main (main.c:432)
==26915==
==26915==
==26915== HEAP SUMMARY:
==26915==     in use at exit: 73,742 bytes in 392 blocks
==26915==   total heap usage: 1,874 allocs, 1,482 frees, 3,253,719 bytes al
==26915==
==26915== LEAK SUMMARY:
==26915==    definitely lost: 0 bytes in 0 blocks
==26915==    indirectly lost: 0 bytes in 0 blocks
==26915==      possibly lost: 151 bytes in 8 blocks
==26915==    still reachable: 73,591 bytes in 384 blocks
==26915==         suppressed: 0 bytes in 0 blocks
==26915== Rerun with --leak-check=full to see details of leaked memory
==26915==
==26915== For counts of detected and suppressed errors, rerun with: -v
==26915== ERROR SUMMARY: 3 errors from 3 contexts (suppressed: 0 from 0)
```

Attachment

poc196min

Impact

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

CVE
CVE-2022-2571
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity

Severity
High (7.8)

Registry
Other

Affected Version
9.0.0047

Visibility
Public

Status
Fixed

Found by
xikhud
@acquykhud
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 533 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

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

We have sent a second follow up to the **vim** team. We will try again in 10 days. 4 months ago

Bram Moolenaar validated this vulnerability 4 months ago

I can reproduce the problem. The POC can be simplified a bit more and ther

xikhud 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 9.0.0101 with commit a6f9e3 4 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Bram Moolenaar 4 months ago

Fixed with patch 9.0.0102

Sign in to join this conversation

Chat with us