Buffer Over-read in function current_quote in vim/vim

0

Valid Reported on Jun 16th 2022

Description

Buffer Over-read in function current_quote at textobject.c:1801

vim version

```
git log
commit 83497f875881973df772cc4cc593766345df6c4a (HEAD -> master, tag: v8.2.
```

POC

```
root@fuzz-vm0-187:/home/fuzz/fuzz/vim/afl/src# ./vim -u NONE -i NONE -n -m
==================================================================
==26523==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6210000
READ of size 1 at 0x621000013d00 thread T0
    #0 0x10c16ec in current_quote /home/fuzz/fuzz/vim/afl/src/textobject.c:
    #1 0xb69bc7 in nv_object /home/fuzz/fuzz/vim/afl/src/normal.c:7105:10
    #2 0xb4b671 in nv_edit /home/fuzz/fuzz/vim/afl/src/normal.c:6884:2
    #3 0xb1f59f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #4 0x814eee in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8808:
    #5 0x814718 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8
    #6 0x8142c9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8689:6
    #7 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #8 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:17
    #9 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:2
    #10 0x115466d in call_user_func_check /home/fuzz/fuzz/v
    #11 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/u
    #12 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
```

#13 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#14 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#15 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#16 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#17 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#18 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#19 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#20 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#21 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#22 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#23 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#24 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#25 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#26 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#27 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#28 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#29 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#30 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#31 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#32 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#33 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#34 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#35 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#36 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#37 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#38 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#39 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#40 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#41 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#42 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#43 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#44 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#45 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#46 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#47 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#48 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#49 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#50 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/
#51 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl
#52 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user

```
#53 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:
#54 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#55 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6

#56 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#57 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#58 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#59 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/useri
#60 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:
#61 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#62 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#63 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#64 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#65 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#66 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/useri
#67 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:
#68 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#69 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#70 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#71 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#72 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#73 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/useri
#74 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:
#75 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#76 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#77 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#78 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#79 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#80 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/useri
#81 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:
#82 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#83 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#84 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#85 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#86 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#87 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/useri
#88 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:
#89 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#90 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/user
#91 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/
#92 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
```

```
#93 0x11585?c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:
#94 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/userf
#95 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612:

#96 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:183
#97 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#98 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
#99 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
#100 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#101 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#102 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#103 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#104 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#105 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#106 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#107 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#108 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#109 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#110 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#111 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#112 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#113 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#114 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#115 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#116 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#117 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#118 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#119 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#120 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#121 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#122 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#123 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#124 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#125 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#126 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#127 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#128 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#129 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#130 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/
#131 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/s
#132 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
```

```
#133 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#134 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992
#135 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c

#136 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#137 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#138 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#139 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#140 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#141 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992
#142 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#143 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#144 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#145 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#146 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#147 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#148 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992
#149 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#150 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#151 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#152 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#153 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#154 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#155 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992
#156 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#157 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#158 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#159 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#160 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#161 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#162 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992
#163 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#164 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#165 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#166 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#167 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#168 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2576
#169 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992
#170 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/
#171 0x115466d in call_user_func_check /home/fuzz/fuzz/
#172 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
```

```
#173 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#174 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#175 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570

#176 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#177 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#178 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#179 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#180 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#181 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#182 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#183 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#184 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#185 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#186 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#187 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#188 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#189 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#190 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#191 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#192 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#193 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#194 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#195 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#196 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#197 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#198 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#199 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#200 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#201 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#202 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#203 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
#204 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
#205 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
#206 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
#207 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
#208 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
#209 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
#210 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/
#211 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src
#212 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
```

```
    #213 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
    #214 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
    #215 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18

    #216 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
    #217 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #218 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #219 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
    #220 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
    #221 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
    #222 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
    #223 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
    #224 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #225 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #226 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
    #227 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
    #228 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
    #229 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
    #230 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
    #231 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #232 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #233 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
    #234 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
    #235 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
    #236 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
    #237 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
    #238 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #239 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #240 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
    #241 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
    #242 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612
    #243 0x114bdb3 in get_func_tv /home/fuzz/fuzz/vim/afl/src/userfunc.c:18
    #244 0x117f4da in ex_call /home/fuzz/fuzz/vim/afl/src/userfunc.c:5593:6
    #245 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #246 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #247 0x115857c in call_user_func /home/fuzz/fuzz/vim/afl/src/userfunc.c
    #248 0x115466d in call_user_func_check /home/fuzz/fuzz/vim/afl/src/user
    #249 0x114ea14 in call_func /home/fuzz/fuzz/vim/afl/src/userfunc.c:3612

0x621000013d00 is located 0 bytes to the right of 4096-byte
allocated by thread T0 here:
```

```
    #0 0x499cad in malloc (/home/fuzz/fuzz/vim/afl/src/vim+0x499cad)
    #1 0x4cb382 in lalloc /home/fuzz/fuzz/vim/afl/src/alloc.c:246:11
    #2 0x4cb26a in alloc /home/fuzz/fuzz/vim/afl/src/alloc.c:151:12

    #3 0x142bfb5 in mf_alloc_bhdr /home/fuzz/fuzz/vim/afl/src/memfile.c:884
    #4 0x142adc7 in mf_new /home/fuzz/fuzz/vim/afl/src/memfile.c:375:26
    #5 0xa60d28 in ml_new_data /home/fuzz/fuzz/vim/afl/src/memline.c:4080:1
    #6 0xa5f6d1 in ml_open /home/fuzz/fuzz/vim/afl/src/memline.c:394:15
    #7 0x501c8a in open_buffer /home/fuzz/fuzz/vim/afl/src/buffer.c:186:9
    #8 0x141ff4c in create_windows /home/fuzz/fuzz/vim/afl/src/main.c:2902:
    #9 0x141e21a in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:711:5
    #10 0x1413dad in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #11 0x7f90cedd6082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/afl/src
Shadow bytes around the buggy address:
  0x0c427fffa750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa790: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fffa7a0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7f0: 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
  ==26523==ABORTING
```

poc_bor1_s.dat

Impact

This vulnerabilities are capable of crashing software, modify Memory, and possible remote execution

CVE
CVE-2022-2124
(Published)

Vulnerability Type
CWE-126: Buffer Over-read

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 895 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. The POC is not usable as a regression test though, because it uses infinite recursion.

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 5 months ago Maintainer

Fixed in patch 8.2.5120

Bram Moolenaar marked this as fixed in **8.2** with commit **2f074f** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation