Use After Free in function qf_fill_buffer in vim/vim

0

✓ Valid Reported on Aug 23rd 2022

Description

Use After Free in function qf_fill_buffer at vim/src/quickfix.c:4790

vim version

```
git log
commit adce965162dd89bf29ee0e5baf53652e7515762c (HEAD -> master, tag: v9.0.
```

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S /home/fuzz/test/poc5_huaf.dat -c :qa!
=================================================================
==27777==ERROR: AddressSanitizer: heap-use-after-free on address 0x60700000
READ of size 4 at 0x6070000028f0 thread T0
    #0 0x56047d532882 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:4790
    #1 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
    #2 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
    #3 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
    #4 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #5 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #6 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #7 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #8 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #9 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #10 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:2886
    #11 0x56047d759189 in call_user_func_check /home/fuzz/v
    #12 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
    #13 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
```

```
#13 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
#14 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
#15 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:477
#16 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
#17 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#18 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#19 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#20 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#21 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#22 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#23 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#24 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#25 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#26 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.
#27 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#28 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
#29 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
#30 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:477
#31 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
#32 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#33 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#34 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#35 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#36 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#37 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#38 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#39 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#40 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#41 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.
#42 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#43 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
#44 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
#45 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:477
#46 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
#47 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#48 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#49 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#50 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#51 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_d
#52 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercm
#53 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#54 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
```

```
#54 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#55 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:2886
#56 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.

#57 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#58 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
#59 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
#60 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:4776
#61 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
#62 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#63 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#64 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#65 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#66 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#67 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#68 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#69 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#70 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:2886
#71 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.
#72 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#73 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
#74 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
#75 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:4776
#76 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
#77 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#78 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#79 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#80 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#81 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#82 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#83 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#84 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#85 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:2886
#86 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.
#87 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#88 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
#89 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
#90 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:4776
#91 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
#92 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/qu
#93 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#94 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
```

```
#94 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#95 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#96 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992

#97 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#98 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#99 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#100 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#101 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc
#102 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#103 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#104 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#105 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#106 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
#107 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#108 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#109 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#110 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#111 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#112 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#113 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#114 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#115 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#116 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc
#117 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#118 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#119 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#120 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#121 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
#122 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#123 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#124 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#125 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#126 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#127 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#128 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#129 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#130 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#131 0x56047d759189 in call_user_func_check /home/fuzz/vi
#132 0x56047d75ba3d in call_func /home/fuzz/vim/src/use
#133 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#134 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
```

```
#134 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#135 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#136 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:

#137 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#138 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#139 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#140 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#141 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#142 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#143 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#144 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#145 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:28
#146 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfun
#147 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#148 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#149 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#150 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#151 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
#152 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#153 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#154 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#155 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#156 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#157 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#158 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#159 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#160 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:28
#161 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfun
#162 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#163 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#164 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#165 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#166 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
#167 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#168 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#169 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#170 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#171 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_
#172 0x56047d745380 in do_ucmd /home/fuzz/vim/src/userc
#173 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#174 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
```

```
#174 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#175 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#176 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc

#177 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#178 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#179 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#180 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#181 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
#182 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#183 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#184 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#185 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#186 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#187 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#188 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#189 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#190 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#191 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc
#192 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#193 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#194 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#195 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#196 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
#197 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
#198 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#199 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
#200 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
#201 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#202 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
#203 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
#204 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
#205 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
#206 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc
#207 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
#208 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
#209 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
#210 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
#211 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/s
#212 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/q
#213 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
#214 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
```

```
    #214 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #215 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #216 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992

    #217 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #218 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #219 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #220 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:28
    #221 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfun
    #222 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
    #223 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
    #224 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
    #225 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
    #226 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
    #227 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
    #228 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
    #229 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #230 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #231 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #232 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #233 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #234 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #235 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:28
    #236 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfun
    #237 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
    #238 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:334
    #239 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:47
    #240 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:47
    #241 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:
    #242 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
    #243 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
    #244 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #245 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #246 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #247 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #248 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #249 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #250 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:28

0x6070000028f0 is located 32 bytes inside of 80-byte region
freed by thread T0 here:
    #0 0x7f206335140f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x56047d13653a in vim_free /home/fuzz/vim/src/alloc.c:625
    #2 0x56047d52e780 in qf_free_items /home/fuzz/vim/src/quickfix.c:3921

    #3 0x56047d52eb2a in qf_free /home/fuzz/vim/src/quickfix.c:3954
    #4 0x56047d524e65 in qf_new_list /home/fuzz/vim/src/quickfix.c:1916
    #5 0x56047d5242fc in qf_init_ext /home/fuzz/vim/src/quickfix.c:1734
    #6 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
    #7 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #8 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #9 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #10 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #11 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #12 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #13 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
    #14 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.
    #15 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
    #16 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
    #17 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:470
    #18 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:477
    #19 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
    #20 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
    #21 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
    #22 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #23 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #24 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #25 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #26 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #27 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #28 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:288
    #29 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.

previously allocated by thread T0 here:
    #0 0x7f2063351808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x56047d13628a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x56047d1360fd in alloc_id /home/fuzz/vim/src/alloc.c:165
    #3 0x56047d5256fb in qf_add_entry /home/fuzz/vim/src/quickfix.c:2113
    #4 0x56047d5240b6 in qf_init_process_nextline /home/fuzz/vim/src/quick
    #5 0x56047d5245c4 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1778
    #6 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quic
    #7 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #8 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #8 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #9 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #10 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892

    #11 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #12 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #13 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:2886
    #14 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.
    #15 0x56047d75ba3d in call_func /home/fuzz/vim/src/userfunc.c:3599
    #16 0x56047d75a2cf in call_callback /home/fuzz/vim/src/userfunc.c:3344
    #17 0x56047d5322b7 in call_qftf_func /home/fuzz/vim/src/quickfix.c:4702
    #18 0x56047d5327b1 in qf_fill_buffer /home/fuzz/vim/src/quickfix.c:4776
    #19 0x56047d5314c4 in qf_update_buffer /home/fuzz/vim/src/quickfix.c:45
    #20 0x56047d5249e5 in qf_init_ext /home/fuzz/vim/src/quickfix.c:1819
    #21 0x56047d5404f3 in cexpr_core /home/fuzz/vim/src/quickfix.c:8015
    #22 0x56047d540828 in ex_cexpr /home/fuzz/vim/src/quickfix.c:8067
    #23 0x56047d2bf5a5 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #24 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #25 0x56047d745380 in do_ucmd /home/fuzz/vim/src/usercmd.c:1892
    #26 0x56047d2bf4da in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2562
    #27 0x56047d2b6848 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #28 0x56047d757f3b in call_user_func /home/fuzz/vim/src/userfunc.c:2886
    #29 0x56047d759189 in call_user_func_check /home/fuzz/vim/src/userfunc.

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/vim/src/quickfix.
Shadow bytes around the buggy address:
  0x0c0e7fff84c0: fd fd fa fa fa fa fd fd fd fd fd fd fd fd fd fd
  0x0c0e7fff84d0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fa fa
  0x0c0e7fff84e0: fa fa fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0e7fff84f0: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fd fd
  0x0c0e7fff8500: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
=>0x0c0e7fff8510: fd fd fd fd fd fd fa fa fa fa fd fd fd fd[fd]fd
  0x0c0e7fff8520: fd fd fd fd fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff8530: 00 00 fa fa fa fa 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff8540: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c0e7fff8550: fa fa 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c0e7fff8560: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
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
  ==27777==ABORTING
```

poc download url:
https://github.com/Janette88/vim/blob/main/poc5_huaf.dat

Impact

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

CVE
CVE-2022-2982
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.6)

Registry
Other

Affected Version
*

Visibility

Public

Status

Fixed

Found by

janette88

@janette88

master

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 891 times.

We are processing your report and will contact the **vim** team within 24 hours. 3 months ago

janette88 modified the report 3 months ago

We have contacted a member of the **vim** team and are waiting to hear back 3 months ago

Bram Moolenaar validated this vulnerability 3 months ago

I can reproduce it, it's deep recursion that causes it.

janette88 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 3 months ago

Fixed with patch 9.0.0260

Chat with us

Bram Moolenaar marked this as fixed in 9.0.0259 with commit d6c676 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation