Heap-based Buffer Overflow in function compile_lock_unlock in vim/vim in vim/vim

0

✓ Valid Reported on Aug 12th 2022

Description

Heap-based Buffer Overflow in function compile_lock_unlock at vim/src/vim9cmds.c:196
#vim version

```
 git log
commit 326c5d36e7cb8526330565109c17b4a13ff790ae (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S poc2_hbo_M.dat -c :qa!
=================================================================
==47794==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000
READ of size 1 at 0x6020000061b6 thread T0
    #0 0x5571726b8dab in compile_lock_unlock /home/fuzz/vim/src/vim9cmds.c:
    #1 0x5571721cc5c1 in ex_unletlock /home/fuzz/vim/src/evalvars.c:1935
    #2 0x5571726b944a in compile_unletlock /home/fuzz/vim/src/vim9cmds.c:26
    #3 0x5571726d7cf3 in compile_def_function /home/fuzz/vim/src/vim9compil
    #4 0x5571726af7f9 in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #5 0x55717220a640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #6 0x5571722018e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #7 0x557172524865 in do_source_ext /home/fuzz/vim/src/scriptfile.c:1674
    #8 0x557172525997 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #9 0x557172522526 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #10 0x55717252258b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #11 0x55717220a640 in do_one_cmd /home/fuzz/vim/src/ex_
    #12 0x5571722018e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #13 0x5571721ffc7d in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #13 0x5571721ffc7d in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #14 0x5571727fba30 in exe_commands /home/fuzz/vim/src/main.c:3133
    #15 0x5571727f4b9e in vim_main2 /home/fuzz/vim/src/main.c:780
    #16 0x5571727f4456 in main /home/fuzz/vim/src/main.c:432
    #17 0x7f5407af7082 in __libc_start_main ../csu/libc-start.c:308
    #18 0x557172081e4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x6020000061b6 is located 0 bytes to the right of 6-byte region [0x60200000
allocated by thread T0 here:
    #0 0x7f5407f8e808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x55717208228a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x55717208207b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x5571725b754d in vim_strsave /home/fuzz/vim/src/strings.c:27
    #4 0x5571726d609c in compile_def_function /home/fuzz/vim/src/vim9compil
    #5 0x5571726af7f9 in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #6 0x55717220a640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #7 0x5571722018e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #8 0x557172524865 in do_source_ext /home/fuzz/vim/src/scriptfile.c:1674
    #9 0x557172525997 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #10 0x557172522526 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #11 0x55717252258b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #12 0x55717220a640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #13 0x5571722018e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #14 0x5571721ffc7d in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #15 0x5571727fba30 in exe_commands /home/fuzz/vim/src/main.c:3133
    #16 0x5571727f4b9e in vim_main2 /home/fuzz/vim/src/main.c:780
    #17 0x5571727f4456 in main /home/fuzz/vim/src/main.c:432
    #18 0x7f5407af7082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim/src/vim9cmds
Shadow bytes around the buggy address:
  0x0c047fff8be0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8bf0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8c00: fa fa 00 00 fa fa 00 00 fa fa 05 fa fa fa fd fa
  0x0c047fff8c10: fa fa fd fa fa fa 00 05 fa fa 06 fa fa fa 02 fa
  0x0c047fff8c20: fa fa 00 05 fa fa fd fa fa fa 02 fa fa fa fd fa
=>0x0c047fff8c30: fa fa 02 fa fa fa[06]fa fa fa fa fa fa fa fa fa
  0x0c047fff8c40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c80: 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
==47794==ABORTING
```

<p><a href="https://github.com/Janette88/vim/blob/main/poc2_hbo_M.dat">poc2_hbo_M.dat</a></p>

Impact

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

CVE
CVE-2022-2819
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity

High (7.8)

Registry

Other

Affected Version

<=v9.0.0194

Visibility

Public

Status

Fixed

Found by

janette88

@janette88

master

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 657 times.

We are processing your report and will contact the **vim** team within 24 hours. 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, POC looks good

janette88 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

Bram Moolenaar 3 months ago Maintainer

Fixed with patch 9.0.0211

Bram Moolenaar marked this as fixed in **9.0.0210** with commit **d1d8f6** 3 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

janette88 3 months ago Researcher

thanks a lot:-) can I have a cve_id for this bug report?

Sign in to join this conversation

Chat with us