Out-of-bounds read in function check_vim9_unlet in vim/vim in vim/vim

0

Valid Reported on Aug 12th 2022

Description

Out-of-bounds read in function check_vim9_unlet at vim/src/vim9cmds.c:95

Vim version

```
git log

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

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S /home/fuzz/test/hbo1_min.dat -c :qa!
=================================================================
==60408==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000(
READ of size 1 at 0x6020000061b4 thread T0
    #0 0x5578cb6533dc in check_vim9_unlet /home/fuzz/vim/src/vim9cmds.c:95
    #1 0x5578cb6538ff in compile_unlet /home/fuzz/vim/src/vim9cmds.c:159
    #2 0x5578cb1675c1 in ex_unletlock /home/fuzz/vim/src/evalvars.c:1935
    #3 0x5578cb6542fe in compile_unletlock /home/fuzz/vim/src/vim9cmds.c:26
    #4 0x5578cb672ba7 in compile_def_function /home/fuzz/vim/src/vim9compil
    #5 0x5578cb64a6ad in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #6 0x5578cb1a5640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #7 0x5578cb19c8e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #8 0x5578cb4bf759 in do_source_ext /home/fuzz/vim/src/sc
    #9 0x5578cb4c088b in do_source /home/fuzz/vim/src/scrip
    #10 0x5578cb4bd41a in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
```

```
    #11 0x5578cb4bd47f in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #12 0x5578cb1a5640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #13 0x5578cb19c8e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992

    #14 0x5578cb19ac7d in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #15 0x5578cb7968e4 in exe_commands /home/fuzz/vim/src/main.c:3133
    #16 0x5578cb78fa52 in vim_main2 /home/fuzz/vim/src/main.c:780
    #17 0x5578cb78f30a in main /home/fuzz/vim/src/main.c:432
    #18 0x7f4ae63b8082 in __libc_start_main ../csu/libc-start.c:308
    #19 0x5578cb01ce4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x6020000061b4 is located 0 bytes to the right of 4-byte region [0x60200006
allocated by thread T0 here:
    #0 0x7f4ae684f808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x5578cb01d28a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x5578cb01d07b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x5578cb552441 in vim_strsave /home/fuzz/vim/src/strings.c:27
    #4 0x5578cb670f50 in compile_def_function /home/fuzz/vim/src/vim9compil
    #5 0x5578cb64a6ad in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #6 0x5578cb1a5640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #7 0x5578cb19c8e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #8 0x5578cb4bf759 in do_source_ext /home/fuzz/vim/src/scriptfile.c:1674
    #9 0x5578cb4c088b in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #10 0x5578cb4bd41a in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #11 0x5578cb4bd47f in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #12 0x5578cb1a5640 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #13 0x5578cb19c8e3 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #14 0x5578cb19ac7d in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #15 0x5578cb7968e4 in exe_commands /home/fuzz/vim/src/main.c:3133
    #16 0x5578cb78fa52 in vim_main2 /home/fuzz/vim/src/main.c:780
    #17 0x5578cb78f30a in main /home/fuzz/vim/src/main.c:432
    #18 0x7f4ae63b8082 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 00 00
  0x0c047fff8c00: fa fa 00 00 fa fa 05 fa fa fa fd fa fa fa fd fa
  0x0c047fff8c10: fa fa fd fa fa fa 04 fa fa fa 04 fa fa fa
  0x0c047fff8c20: fa fa fd fa fa fa 02 fa fa fa 01 fa fa fa
=>0x0c047fff8c30: fa fa 01 fa fa fa[04]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 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
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
==60408==ABORTING
```

Download POC: hbo1_min.dat

Impact

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

CVE
CVE-2022-2816
(Published)

(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

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 647 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

janette88 modified the report 3 months ago

janette88 modified the report 3 months ago

We have contacted a member of the **vim** team and are waiting to hear bac

Bram Moolenaar validated this vulnerability 3 months ago

I can reproduce it. The POC can be simplified, only "unlet" is needed inside the function.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar marked this as fixed in 9.0.0211 with commit dbdd16 3 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Bram Moolenaar 3 months ago Maintainer

Fixed with patch 9.0.0212

Sign in to join this conversation

FAQ

contact us

terms

privacy policy