use after free in function generate_PCALL in vim/vim

0

Valid Reported on Aug 14th 2022

Description

Use After Free in function generate_PCALL at vim/src/vim9instr.c:1606

vim version

```
git log
commit 249e1b903a9c0460d618f6dcc59aeb8c03b24b20 (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S poc2_huaf.dat -c :qa!
==================================================================
==66407==ERROR: AddressSanitizer: heap-use-after-free on address 0x60300000
READ of size 4 at 0x603000000e80 thread T0
    #0 0x5577ee9343b7 in generate_PCALL /home/fuzz/vim/src/vim9instr.c:1606
    #1 0x5577ee920177 in compile_call /home/fuzz/vim/src/vim9expr.c:890
    #2 0x5577ee9284ba in compile_expr9 /home/fuzz/vim/src/vim9expr.c:2360
    #3 0x5577ee928a3c in compile_expr8 /home/fuzz/vim/src/vim9expr.c:2420
    #4 0x5577ee928c61 in compile_expr7 /home/fuzz/vim/src/vim9expr.c:2454
    #5 0x5577ee92963a in compile_expr6 /home/fuzz/vim/src/vim9expr.c:2533
    #6 0x5577ee92a426 in compile_expr5 /home/fuzz/vim/src/vim9expr.c:2641
    #7 0x5577ee92b070 in compile_expr4 /home/fuzz/vim/src/vim9expr.c:2778
    #8 0x5577ee92cdf1 in compile_expr3 /home/fuzz/vim/src/vim9expr.c:3052
    #9 0x5577ee92ce93 in compile_expr2 /home/fuzz/vim/src/vim9expr.c:3077
    #10 0x5577ee92d0e5 in compile_expr1 /home/fuzz/vim/src/vim9expr.c:3118
    #11 0x5577ee92e315 in compile_expr0_ext /home/fuzz/vim/
    #12 0x5577ee92e574 in compile_expr0 /home/fuzz/vim/src/v
    #13 0x5577ee8d55b4 in compile_eval /home/fuzz/vim/src/vim9cmds.c:1669
```

```
    #14 0x5577ee8ec4ee in compile_def_function /home/fuzz/vim/src/vim9compi
    #15 0x5577ee8c38d8 in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #16 0x5577ee41e443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #17 0x5577ee4156e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #18 0x5577ee738845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #19 0x5577ee739977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #20 0x5577ee736506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #21 0x5577ee73656b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #22 0x5577ee41e443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #23 0x5577ee4156e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #24 0x5577ee413a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #25 0x5577eea0feda in exe_commands /home/fuzz/vim/src/main.c:3133
    #26 0x5577eea09048 in vim_main2 /home/fuzz/vim/src/main.c:780
    #27 0x5577eea08900 in main /home/fuzz/vim/src/main.c:432
    #28 0x7f741c48d082 in __libc_start_main ../csu/libc-start.c:308
    #29 0x5577ee294e4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x603000000e80 is located 0 bytes inside of 24-byte region [0x603000000e80,
freed by thread T0 here:
    #0 0x7f741c92440f in __interceptor_free ../../../../src/libsanitizer/as
    #1 0x5577ee29553a in vim_free /home/fuzz/vim/src/alloc.c:625
    #2 0x5577ee93d169 in clear_type_list /home/fuzz/vim/src/vim9type.c:47
    #3 0x5577ee8b31a6 in func_clear_items /home/fuzz/vim/src/userfunc.c:236
    #4 0x5577ee8b34e6 in func_clear /home/fuzz/vim/src/userfunc.c:2400
    #5 0x5577ee8b3708 in func_clear_free /home/fuzz/vim/src/userfunc.c:2437
    #6 0x5577ee8c4e28 in func_ptr_unref /home/fuzz/vim/src/userfunc.c:5371
    #7 0x5577ee8de71c in compile_nested_function /home/fuzz/vim/src/vim9com
    #8 0x5577ee8ebc95 in compile_def_function /home/fuzz/vim/src/vim9compil
    #9 0x5577ee8c38d8 in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #10 0x5577ee41e443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #11 0x5577ee4156e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #12 0x5577ee738845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #13 0x5577ee739977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #14 0x5577ee736506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #15 0x5577ee73656b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #16 0x5577ee41e443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #17 0x5577ee4156e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #18 0x5577ee413a80 in do_cmdline_cmd /home/fuzz/vim/src/
    #19 0x5577eea0feda in exe_commands /home/fuzz/vim/src/m
    #20 0x5577eea09048 in vim_main2 /home/fuzz/vim/src/main.c:780
```

```
    #21 0x5577eea08900 in main /home/fuzz/vim/src/main.c:432
    #22 0x7f741c48d082 in __libc_start_main ../csu/libc-start.c:308


previously allocated by thread T0 here:
    #0 0x7f741c924808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x5577ee29528a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x5577ee295120 in alloc_clear /home/fuzz/vim/src/alloc.c:177
    #3 0x5577ee93cff7 in get_type_ptr /home/fuzz/vim/src/vim9type.c:34
    #4 0x5577ee93e26c in alloc_func_type /home/fuzz/vim/src/vim9type.c:234
    #5 0x5577ee8ee0a9 in set_function_type /home/fuzz/vim/src/vim9compile.c
    #6 0x5577ee8c2749 in define_function /home/fuzz/vim/src/userfunc.c:4956
    #7 0x5577ee8de1e3 in compile_nested_function /home/fuzz/vim/src/vim9com
    #8 0x5577ee8ebc95 in compile_def_function /home/fuzz/vim/src/vim9compil
    #9 0x5577ee8c38d8 in ex_defcompile /home/fuzz/vim/src/userfunc.c:5098
    #10 0x5577ee41e443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #11 0x5577ee4156e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #12 0x5577ee738845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #13 0x5577ee739977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #14 0x5577ee736506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #15 0x5577ee73656b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #16 0x5577ee41e443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #17 0x5577ee4156e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #18 0x5577ee413a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #19 0x5577eea0feda in exe_commands /home/fuzz/vim/src/main.c:3133
    #20 0x5577eea09048 in vim_main2 /home/fuzz/vim/src/main.c:780
    #21 0x5577eea08900 in main /home/fuzz/vim/src/main.c:432
    #22 0x7f741c48d082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-use-after-free /home/fuzz/vim/src/vim9instr
Shadow bytes around the buggy address:
  0x0c067fff8180: fa fa 00 00 04 fa fa fa 00 00 00 01 fa fa 00 00
  0x0c067fff8190: 00 fa fa fa 00 00 00 fa fa fa 00 00 01 fa fa fa
  0x0c067fff81a0: 00 00 00 06 fa fa fd fd fd fd fa fa 00 00 00 06
  0x0c067fff81b0: fa fa 00 00 00 06 fa fa 00 00 00 06 fa fa fd fd
  0x0c067fff81c0: fd fa fa fa fd fd fd fa fa fa fd fd fd fd fa fa
=>0x0c067fff81d0:[fd]fd fd fa fa fa fd fd fd fd fa fa fd fd fd fd
  0x0c067fff81e0: fa fa fd fd fd fd fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c067fff8220: 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
==66407==ABORTING
```

poc2_huaf.dat

Impact

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

CVE
CVE-2022-2862
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity
High (7.6)

Registry
Other

Affected Version
<=v9.0.0213

Visibility
Public

Status
Fixed

Found by
janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 774 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 this.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 3 months ago Maintainer

Fixed with patch 9.0.0221

Bram Moolenaar marked this as fixed in 9.0.0220 with commit 1889f4 3 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation