

heap-use-after-free in function find_pattern_in_path in vim/vim

0



Valid

Reported on May 16th 2022

Description

heap-use-after-free in function find_pattern_in_path at search.c:3683

vim version

git log

commit 5a8fad32ea9c075f045b37d6c7739891d458f82b (HEAD -> master, tag: v8.2.0)



POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /mnt/share/max/fuzz/poc/vim/poc_
=====
==15953==ERROR: AddressSanitizer: heap-use-after-free on address 0x60200000
READ of size 1 at 0x602000007dd0 thread T0
#0 0x431c9e in strcmp (/home/fuzz/fuzz/vim/vim/src/vim+0x431c9e)
#1 0xe84626 in find_pattern_in_path /home/fuzz/fuzz/vim/vim/src/search.c:3683
#2 0x12a5572 in do_window /home/fuzz/fuzz/vim/vim/src/window.c:582:3
#3 0xb3cdfc in nv_window /home/fuzz/fuzz/vim/vim/src/normal.c:5614:2
#4 0xb1a341 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
#5 0x80ebde in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8757:1
#6 0x80e408 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8757:1
#7 0x80dfb9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8638:6
#8 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:1
#9 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:1
#10 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:1
#11 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:1
```

Chat with us

```
#12 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
#13 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1206
#14 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
#15 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
#16 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:9
#17 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
#18 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
#19 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
#20 0x7fbd2aa91082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
#21 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)
```

0x602000007dd0 is located 0 bytes inside of 2-byte region [0x602000007dd0,0x602000007dd2), freed by thread T0 here:

```
#0 0x499a62 in free (/home/fuzz/fuzz/vim/vim/src/vim+0x499a62)
#1 0x4cbe06 in vim_free /home/fuzz/fuzz/vim/vim/src/alloc.c:621:2
#2 0xa5f095 in ml_flush_line /home/fuzz/fuzz/vim/vim/src/memline.c:406:5
#3 0xa74895 in ml_get_buf /home/fuzz/fuzz/vim/vim/src/memline.c:2651:2
#4 0xa709f9 in ml_get /home/fuzz/fuzz/vim/vim/src/memline.c:2564:12
#5 0xe81c83 in find_pattern_in_path /home/fuzz/fuzz/vim/vim/src/search.c:103:1
#6 0x12a5572 in do_window /home/fuzz/fuzz/vim/vim/src/window.c:582:3
#7 0xb3cdfc in nv_window /home/fuzz/fuzz/vim/vim/src/normal.c:5614:2
#8 0xb1a341 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
#9 0x80ebde in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8757:1
#10 0x80e408 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8757:1
#11 0x80dfb9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8638:6
#12 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:1
#13 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
#14 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:1
#15 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:1
#16 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
#17 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1206
#18 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:1
#19 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
#20 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:9
#21 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
#22 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
#23 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
#24 0x7fbd2aa91082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
```

Chat with us

previously allocated by thread T0 here:

```
#0 0x499a62 in free (/home/fuzz/fuzz/vim/vim/src/vim+0x499a62)
```

```

#0 0x499ccd in malloc (/home/fuzz/fuzz/vim/vim/src/vim+0x499ccd)
#1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
#2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12

#3 0x54947d in ins_char_bytes /home/fuzz/fuzz/vim/vim/src/change.c:109:
#4 0x549f4b in ins_char /home/fuzz/fuzz/vim/vim/src/change.c:1007:5
#5 0x692d3f in insertchar /home/fuzz/fuzz/vim/vim/src/edit.c:2297:6
#6 0x68add9 in insert_special /home/fuzz/fuzz/vim/vim/src/edit.c:2056:2
#7 0x6705c7 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1375:3
#8 0xb649ec in invoke_edit /home/fuzz/fuzz/vim/vim/src/normal.c:7028:9
#9 0xb66704 in n_opencmd /home/fuzz/fuzz/vim/vim/src/normal.c:6275:6
#10 0xb4ceb6 in nv_open /home/fuzz/fuzz/vim/vim/src/normal.c:7409:2
#11 0xb1a341 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
#12 0x80ebde in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:875:
#13 0x80e408 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:
#14 0x80dfb9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8638:6
#15 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
#16 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
#17 0xe5191c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
#18 0xe4e376 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:
#19 0xe4dcac in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117:
#20 0xe4d38e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1206:
#21 0x7d7529 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:
#22 0x7c42e5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
#23 0x7c8f31 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
#24 0x1419502 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3108:2
#25 0x141569b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
#26 0x140ad95 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
#27 0x7fbd2aa91082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

```

SUMMARY: AddressSanitizer: heap-use-after-free (/home/fuzz/fuzz/vim/vim/src
Shadow bytes around the buggy address:

```

0x0c047fff8f60: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd
0x0c047fff8f70: fa fa fd fd fa fa fd fd fa fa fd fa fa fa fd fd
0x0c047fff8f80: fa fa fd fd fa fa fd fd fa fa fd fa fa fa fd fd
0x0c047fff8f90: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fff8fa0: fa fa fd fd fa fa fd fd fa fa fd fa fa fa 01 fa
=>0x0c047fff8fb0: fa fa 00 00 fa fa 01 fa fa fa[fd]fa fa fa 05 fa
0x0c047fff8fc0: fa fa 02 fa fa fa 01 fa fa fa 00 00 fa fa 00 00
0x0c047fff8fd0: fa fa 06 fa fa fa 06 fa fa fa 06 fa fa fa
0x0c047fff8fe0: fa fa 01 fa fa fa 06 fa fa fa 01 fa fa fa 01 fa
0x0c047fff8ff0: fa fa 00 fa fa fa 00 fa fa fa 00 fa fa fa 00 fa

```

Chat with us

0x0c04/+++8++0: ta ta ta ta ta ta ta ta ta ta ta ta ta ta ta ta
0x0c047fff9000: 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
==15953==ABORTING



[poc_huaf_s.dat](#)

Impact

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

CVE
CVE-2022-1796
(Published)

Vulnerability Type
CWE-416: Use After Free

Severity

Chat with us

Severity
Medium (6.6)


Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by
TDHX ICS Security
@jieyongma
pro ▾

Fixed by
 Bram Moolenaar
@brammool
maintainer

This report was seen 829 times.

We are processing your report and will contact the **vim** team within 24 hours. 6 months ago

We have contacted a member of the **vim** team and are waiting to hear back 6 months ago

Bram Moolenaar 6 months ago

Maintainer

I can see the problem, but the POC is incomplete - the "vszs" command splits off a window to edit src/if_mzscheme.c, and depends on its contents. When run in another directory the result will be different.

Bram Moolenaar 6 months ago

Chat with us

Never mind. I found a simple file contents to reproduce the problem

never mind, found a simple file contents to reproduce the problem.

Bram Moolenaar validated this vulnerability 6 months ago

Instead of opening the if_mzsch.c file using a generated file the repro steps are reliable.

TDHX ICS Security has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 6 months ago

Maintainer

Fixed in patch 8.2.4979

Bram Moolenaar marked this as fixed in 8.2 with commit 28d032 6 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ren0216 5 months ago

At commit 5a8fad32, this poc still could not reproduce the problem, so what can I do? Can't stop thinking there is something wrong in the poc.

Bram Moolenaar 5 months ago

Maintainer

Not sure if there is a remaining problem. This issue is fixed and closed. If you see another problem, or can still reproduce a similar issue, please create a new item.

Sign in to join this conversation

Chat with us

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)

[Chat with us](#)