Stack-based Buffer Overflow in function ex_finally in vim/vim

0

Valid Reported on Sep 22nd 2022

Description

stack-buffer-overflow in ex_finally function

Proof of Concept

https://raw.githubusercontent.com/xiowane/testfile/main/test

ASAN

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /src/results/crashes/test -c :qa
=================================================================
==316==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffed0ac
READ of size 2 at 0x7ffed0ad1d3e thread T0
    #0 0x55cfb2a25f1b in ex_finally /src/src/ex_eval.c:1956:6
    #1 0x55cfb29b8606 in do_one_cmd /src/src/ex_docmd.c:2569:2
    #2 0x55cfb29b8606 in do_cmdline /src/src/ex_docmd.c:990:17
    #3 0x55cfb313b072 in do_source_ext /src/src/scriptfile.c:1667:5
    #4 0x55cfb314d1ae in do_source /src/src/scriptfile.c:1811:12
    #5 0x55cfb314d1ae in cmd_source /src/src/scriptfile.c:1163:14
    #6 0x55cfb314d1ae in ex_source /src/src/scriptfile.c:1189:2
    #7 0x55cfb29b8606 in do_one_cmd /src/src/ex_docmd.c:2569:2
    #8 0x55cfb29b8606 in do_cmdline /src/src/ex_docmd.c:990:17
    #9 0x55cfb37d96d8 in do_cmdline_cmd /src/src/ex_docmd.c:584:12
    #10 0x55cfb37d96d8 in exe_commands /src/src/main.c:3139:2
    #11 0x55cfb37d96d8 in vim_main2 /src/src/main.c:781:2
    #12 0x55cfb37d13ca in main /src/src/main.c:432:12
    #13 0x7f1adb39cd8f  (/lib/x86_64-linux-gnu/libc.so.6+0x
    #14 0x7f1adb39ce3f in __libc_start_main (/lib/x86_64-li
    #15 0x55cfb2512344 in _start (/src/src/vim+0x2d5344) (BuildId: 1061b751
```

```
Address 0x7ffed0ad1d3e is located in stack of thread T0 at offset 670 in fr
    #0 0x55cfb29a37af in do_cmdline /src/src/ex_docmd.c:624


  This frame has 9 object(s):
    [32, 36) 'bad_char_idx.i' (line 5397)
    [48, 56) 'errormsg.i' (line 1730)
    [80, 264) 'ea.i' (line 1732)
    [336, 576) 'save_cmdmod.i' (line 1733)
    [640, 648) 'cmdline_copy' (line 626)
    [672, 2256) 'cstack' (line 634) <== Memory access at offset 670 underfl
    [2384, 2408) 'lines_ga' (line 635)
    [2448, 2456) 'private_msg_list' (line 644)
    [2480, 2512) 'cmd_loop_cookie' (line 649)
HINT: this may be a false positive if your program uses some custom stack u
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /src/src/ex_eval.c:1956:6
Shadow bytes around the buggy address:
  0x10005a152350: 00 00 00 00 f1 f1 f1 f1 f8 f2 00 f2 f2 f2 00 00
  0x10005a152360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005a152370: 00 00 00 00 00 f2 f2 f2 f2 f2 f2 f2 f2 f2 00 00
  0x10005a152380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005a152390: 00 00 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 f2
=>0x10005a1523a0: f2 f2 f2 f2 00 f2 f2[f2]00 00 00 00 00 00 00 00
  0x10005a1523b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005a1523c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005a1523d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005a1523e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10005a1523f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
  ==316==ABORTING
```

Impact

This vulnerability is capable of arbitrary code execution.

References

- poc

CVE
CVE-2022-3296
(Published)

Vulnerability Type
CWE-121: Stack-based Buffer Overflow

Severity
High (7.8)

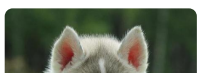
Registry
Other

Affected Version
9.0.0538

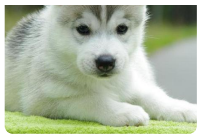
Visibility
Public

Status
Fixed

Found by



xiowane



@xiowane

unranked

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,355 times.

We are processing your report and will contact the **vim** team within 24 hours. 2 months ago

We have contacted a member of the **vim** team and are waiting to hear back 2 months ago

Bram Moolenaar validated this vulnerability 2 months ago

I can reproduce it. Only fails with ASAN, not with valgrind.

xiowane 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 **9.0.0577** with commit **96b9bf** 2 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

Chat with us