huntr

heap-buffer-overflow occurs in function eval_string ./vim/src/typval.c:2226 in vim/vim

0

✓ Valid Reported on Jul 20th 2022

Description

heap-buffer-overflow occurs in eval_string ./vim/src/typval.c:2226, it should be allocated more memory at ./vim/src/typval.c:2126

vim version

```
git log
commit 5154a8880034b7bb94186d37bcecc6ee1a96f732 (HEAD -> master, tag: v9.0.
```

Proof of Concept

Poc

```
# ./vim -u NONE -i NONE -n -m -X -Z -e -s -S ./vim-poc-min

==2558612==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6030(
WRITE of size 1 at 0x603000000cb8 thread T0
    #0 0x5634a09bf8fd in eval_string /src/vim/src/typval.c:2226:10
    #1 0x5634a09c406e in eval_interp_string /src/vim/src/typval.c:2349:12
    #2 0x56349ec66fcf in eval9 /src/vim/src/eval.c:3929:13
    #3 0x56349ec8477f in eval8 /src/vim/src/eval.c:3602:11
    #4 0x56349ec7fc41 in eval7 /src/vim/src/eval.c:3394:9
    #5 0x56349ec7d007 in eval6 /src/vim/src/eval.c:3235:6
    #6 0x56349ec7613b in eval5 /src/vim/src/eval.c:3046:9
    #7 0x56349ec72c5f in eval4 /src/vim/src/eval.c:2897:9
    #8 0x56349ec6f4a8 in eval3 /src/vim/src/eval.c:2758:9
    #9 0x56349ec10fd8 in eval2 /src/vim/src/eval.c:2632:9
```

Chat with us

```
    #9 0x56349ec10fd8 in eval2 /src/vim/src/eval.c:2632:9
    #10 0x56349ebc2361 in eval1 /src/vim/src/eval.c:2478:9
    #11 0x56349e998e3d in eval_dict /src/vim/src/dict.c:955:10
    #12 0x56349ec6698a in eval9 /src/vim/src/eval.c:3915:13
    #13 0x56349ec8477f in eval8 /src/vim/src/eval.c:3602:11
    #14 0x56349ec7fc41 in eval7 /src/vim/src/eval.c:3394:9
    #15 0x56349ec79868 in eval6 /src/vim/src/eval.c:3157:9
    #16 0x56349ec7613b in eval5 /src/vim/src/eval.c:3046:9
    #17 0x56349ec72c5f in eval4 /src/vim/src/eval.c:2897:9
    #18 0x56349ec6f4a8 in eval3 /src/vim/src/eval.c:2758:9
    #19 0x56349ec10fd8 in eval2 /src/vim/src/eval.c:2632:9
    #20 0x56349ebc2361 in eval1 /src/vim/src/eval.c:2478:9
    #21 0x56349ec59884 in ex_echo /src/vim/src/eval.c:6629:6
    #22 0x56349ef01e6c in do_one_cmd /src/vim/src/ex_docmd.c:2570:2
    #23 0x56349eed94e0 in do_cmdline /src/vim/src/ex_docmd.c:992:17
    #24 0x5634a014d7f4 in do_source_ext /src/vim/src/scriptfile.c:1674:5
    #25 0x5634a0145055 in do_source /src/vim/src/scriptfile.c:1801:12
    #26 0x5634a0144464 in cmd_source /src/vim/src/scriptfile.c:1174:14
    #27 0x5634a0142ed1 in ex_source /src/vim/src/scriptfile.c:1200:2
    #28 0x56349ef01e6c in do_one_cmd /src/vim/src/ex_docmd.c:2570:2
    #29 0x56349eed94e0 in do_cmdline /src/vim/src/ex_docmd.c:992:17
    #30 0x56349eee23e0 in do_cmdline_cmd /src/vim/src/ex_docmd.c:586:12
    #31 0x5634a13b0267 in exe_commands /src/vim/src/main.c:3133:2
    #32 0x5634a13a5b60 in vim_main2 /src/vim/src/main.c:780:2
    #33 0x5634a1384e19 in main /src/vim/src/main.c:432:12
    #34 0x7f1f31a72d8f  (/lib/x86_64-linux-gnu/libc.so.6+0x29d8f) (BuildId:
    #35 0x7f1f31a72e3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #36 0x56349e5b5ab4 in _start (/src/vim/src/vim+0xa08ab4) (BuildId: 0e0

0x603000000cb8 is located 0 bytes to the right of 24-byte region [0x603000
allocated by thread T0 here:
    #0 0x56349e6388fe in __interceptor_malloc (/src/vim/src/vim+0xa8b8fe) (
    #1 0x56349e673dfb in lalloc /src/vim/src/alloc.c:246:11
    #2 0x56349e673cf9 in alloc /src/vim/src/alloc.c:151:12
    #3 0x5634a09b8d7b in eval_string /src/vim/src/typval.c:2126:28
    #4 0x5634a09c406e in eval_interp_string /src/vim/src/typval.c:2349:12
    #5 0x56349ec66fcf in eval9 /src/vim/src/eval.c:3929:13
    #6 0x56349ec8477f in eval8 /src/vim/src/eval.c:3602:11
    #7 0x56349ec7fc41 in eval7 /src/vim/src/eval.c:3394:9
    #8 0x56349ec7d007 in eval6 /src/vim/src/eval.c:3235:6
    #9 0x56349ec7613b in eval5 /src/vim/src/eval.c:3046:9
    #10 0x56349ec72c5f in eval4 /src/vim/src/eval.c:2897:9
    #10 0x56349ec72c5f in eval4 /src/vim/src/eval.c:2897:9
    #11 0x56349ec6f4a8 in eval3 /src/vim/src/eval.c:2758:9
    #12 0x56349ec10fd8 in eval2 /src/vim/src/eval.c:2632:9

    #13 0x56349ebc2361 in eval1 /src/vim/src/eval.c:2478:9
    #14 0x56349e998e3d in eval_dict /src/vim/src/dict.c:955:10
    #15 0x56349ec6698a in eval9 /src/vim/src/eval.c:3915:13
    #16 0x56349ec8477f in eval8 /src/vim/src/eval.c:3602:11
    #17 0x56349ec7fc41 in eval7 /src/vim/src/eval.c:3394:9
    #18 0x56349ec79868 in eval6 /src/vim/src/eval.c:3157:9
    #19 0x56349ec7613b in eval5 /src/vim/src/eval.c:3046:9
    #20 0x56349ec72c5f in eval4 /src/vim/src/eval.c:2897:9
    #21 0x56349ec6f4a8 in eval3 /src/vim/src/eval.c:2758:9
    #22 0x56349ec10fd8 in eval2 /src/vim/src/eval.c:2632:9
    #23 0x56349ebc2361 in eval1 /src/vim/src/eval.c:2478:9
    #24 0x56349ec59884 in ex_echo /src/vim/src/eval.c:6629:6
    #25 0x56349ef01e6c in do_one_cmd /src/vim/src/ex_docmd.c:2570:2
    #26 0x56349eed94e0 in do_cmdline /src/vim/src/ex_docmd.c:992:17
    #27 0x5634a014d7f4 in do_source_ext /src/vim/src/scriptfile.c:1674:5
    #28 0x5634a0145055 in do_source /src/vim/src/scriptfile.c:1801:12
    #29 0x5634a0144464 in cmd_source /src/vim/src/scriptfile.c:1174:14

SUMMARY: AddressSanitizer: heap-buffer-overflow /src/vim/src/typval.c:2226:
Shadow bytes around the buggy address:
  0x0c067fff8140: 00 00 00 00 fa fa 00 00 00 00 fa fa 00 00 01 fa
  0x0c067fff8150: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8160: fd fa fa fa 00 00 00 02 fa fa fd fd fd fd fa fa
  0x0c067fff8170: 00 00 00 02 fa fa 00 00 00 fa fa fa fd fd fd fd
  0x0c067fff8180: fa fa 00 00 00 fa fa fa 00 00 00 02 fa fa 00 00
=>0x0c067fff8190: 00 fa fa fa 00 00 00[fa]fa fa fa fa fa fa fa fa
  0x0c067fff81a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff81e0: 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 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
  ==2558612==ABORTING
```

Impact

This may result in corruption of sensitive information, a crash, or code execution among other things.

CVE
CVE-2022-2580
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.3)

Registry
Other

Affected Version
commit 5154a8880034b7bb94186d37bcecc6ee1a96f732

Visibility
Public

Status
Fixed

Found by

Ender

@enderdzz

unranked

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 542 times.

We are processing your report and will contact the **vim** team within 24 hours. 4 months ago

We have contacted a member of the **vim** team and are waiting to hear back 4 months ago

We have sent a follow up to the **vim** team. We will try again in 7 days. 4 months ago

Ender modified the report 4 months ago

Bram Moolenaar validated this vulnerability 4 months ago

I can reproduce it. The POC can be simplified a little.

Ender has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 4 months ago

Maintainer

Fixed with patch 9.0.0104

Bram Moolenaar marked this as fixed in **9.0.0102** with commit **1e56bd** 4 m

Chat with us

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

juweihuitao 4 months ago

Can you post the poc?

Bram Moolenaar 4 months ago Maintainer

Patch 9.0.0104 has a regression test.

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us