# Heap-based Buffer Overflow in vim/vim

✓ Valid Reported on Nov 12th 2021

0

**Description**

Greetings,

A Heap-based Buffer Overflow issue was discovered in Vim.

The POC file is reduced to the absolute minimum to reproduce the problem. Please see sanitizer output and the "trimmed" POC file link below.

**System info** OS version : Ubuntu 20.04.2 LTS + Clang 12 with ASan Vim Version : master(58ef8a3) - Fri Nov 12 11:25:11 2021 +0000

**Steps to reproduce:**

```
git clone https://github.com/vim/vim
```

```
LD=lld-12 AS=llvm-as-12 AR=llvm-ar-12 RANLIB=llvm-ranlib-12 CC=clang-12 CX
```

Download POC from This URL

```
./vim -u NONE -X -Z -e -s -S POC -c :qa!
```

Sanitizer output:

```
=================================================================
==135716==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100
READ of size 1 at 0x621000012900 thread T0
    #0 0xaccc0d in grab_file_name /src/fuzzer11/triage_yeni/vim/src/findfil
    #1 0x19b3220 in do_window /src/fuzzer11/triage_yeni/vim/src/window.c:52
    #2 0xe845de in normal_cmd /src/fuzzer11/triage_yeni/vim/src/normal.c:1
    #3 0x9aefb4 in exec_normal /src/fuzzer11/triage_yeni/vim/src/ex_docmd.
    #4 0x9ad0aa in exec_normal_cmd /src/fuzzer11/triage_yeni/vim/src/ex_do
    #5 0x9ad0aa in ex_normal /src/fuzzer11/triage_yeni/vim/src/ex_docmd.c:
    #6 0x94ff7b in do_one_cmd /src/fuzzer11/triage_yeni/vim/src/ex_docmd.c:
    #7 0x94ff7b in do_cmdline /src/fuzzer11/triage_yeni/vim/src/ex_docmd.c:
    #8 0x5064ee in apply_autocmds_group /src/fuzzer11/triage_yeni/vim/src/
    #9 0x50da64 in apply_autocmds /src/fuzzer11/triage_yeni/vim/src/autocm
    #10 0x52a0f5 in buf_freeall /src/fuzzer11/triage_yeni/vim/src/buffer.c:
    #11 0x531471 in buflist_new /src/fuzzer11/triage_yeni/vim/src/buffer.c:
    #12 0x55c374 in buflist_add /src/fuzzer11/triage_yeni/vim/src/buffer.c:
    #13 0x4d88c7 in alist_add /src/fuzzer11/triage_yeni/vim/src/arglist.c:
    #14 0x4d88c7 in alist_set /src/fuzzer11/triage_yeni/vim/src/arglist.c:1
    #15 0x4dbf91 in do_arglist /src/fuzzer11/triage_yeni/vim/src/arglist.c:
    #16 0x4e1aba in ex_next /src/fuzzer11/triage_yeni/vim/src/arglist.c:751
    #17 0x94ff7b in do_one_cmd /src/fuzzer11/triage_yeni/vim/src/ex_docmd.
    #18 0x94ff7b in do_cmdline /src/fuzzer11/triage_yeni/vim/src/ex_docmd.
    #19 0x136cde4 in do_source /src/fuzzer11/triage_yeni/vim/src/scriptfil
    #20 0x13699e1 in cmd_source /src/fuzzer11/triage_yeni/vim/src/scriptfi
    #21 0x13699e1 in ex_source /src/fuzzer11/triage_yeni/vim/src/scriptfil
    #22 0x94ff7b in do_one_cmd /src/fuzzer11/triage_yeni/vim/src/ex_docmd.
    #23 0x94ff7b in do_cmdline /src/fuzzer11/triage_yeni/vim/src/ex_docmd.
    #24 0x1bcecfc in exe_commands /src/fuzzer11/triage_yeni/vim/src/main.c:
    #25 0x1bcecfc in vim_main2 /src/fuzzer11/triage_yeni/vim/src/main.c:77
    #26 0x1bc5a8f in main /src/fuzzer11/triage_yeni/vim/src/main.c:425:12
    #27 0x7f9daa6ad0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #28 0x41f64d in _start (/src/fuzzer11/triage_yeni/vim/src/vim+0x41f64d)

0x621000012900 is located 0 bytes to the right of 4096-byte region [0x6210
allocated by thread T0 here:
    #0 0x49a8ad in malloc (/src/fuzzer11/triage_yeni/vim/src/vim+0x49a8ad)
    #1 0x4cc2cb in lalloc /src/fuzzer11/triage_yeni/vim/src/alloc.c:244:11

SUMMARY: AddressSanitizer: heap-buffer-overflow /src/fuzzer11/triage_yeni/
Shadow bytes around the buggy address:
  0x0c427fffa4d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa4e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa4f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa500: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa510: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fffa520:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa530: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa540: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa550: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa560: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa570: 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
```

(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.5)

Visibility
Public

Status
Fixed

Found by

cem
@cemonatk
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

```
  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
        alloca redzone:    cb
      w gap:               cc
     6==ABORTING
```

s:
Heap-based Buffer Overflow - https://cwe.mitre.org/data/definitions/122.html
This vulnerability is capable of crashing software, bypass protection mechanism, modify of memory, and successful exploitation may lead to code execution

This report was seen 933 times.

## References

Cem Onat Karagun

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

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

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

Bram Moolenaar a year ago Maintainer

I can reproduce it.

Bram Moolenaar validated this vulnerability a year ago

cem has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar a year ago Maintainer

Fix is in patch 8.2.3611, please verify

cem a year ago Researcher

Looks good - tested with patch 8.2.3616.

Bram Moolenaar marked this as fixed with commit 615ddd a year ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

CVE published! 🎊

Jamie Slome a year ago Admin

@ cemonatk 👋 it looks like a bug on our side caused the disclosure bounty to be set to $355 erroneously. We have restored it to the reward shown at the point of disclosure ($0). We apologize for the inconvenience or confusion caused.

Sign in to join this conversation