Heap-based Buffer Overflow in function latin_ptr2len in vim/vim

0

Valid Reported on Aug 14th 2022

Description

Heap-based Buffer Overflow in function latin_ptr2len at vim/src/mbyte.c:1088 .

vim version

```
git log
commit 249e1b903a9c0460d618f6dcc59aeb8c03b24b20 (grafted, HEAD -> master, t
```

Proof of Concept

```
./vim -u NONE -X -Z -e -s -S poc4_hbo.dat -c :qa!
==================================================================
==66771==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000(
READ of size 1 at 0x602000006111 thread T0
    #0 0x55ec6e7efd5d in latin_ptr2len /home/fuzz/vim/src/mbyte.c:1088
    #1 0x55ec6e6341e4 in next_for_item /home/fuzz/vim/src/eval.c:1852
    #2 0x55ec6e6f1e21 in ex_while /home/fuzz/vim/src/ex_eval.c:1304
    #3 0x55ec6e6c2443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #4 0x55ec6e6b96e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #5 0x55ec6e9dc845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:167
    #6 0x55ec6e9dd977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #7 0x55ec6e9da506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #8 0x55ec6e9da56b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #9 0x55ec6e6c2443 in do_one_cmd /home/fuzz/vim/src/ex_do
    #10 0x55ec6e6b96e6 in do_cmdline /home/fuzz/vim/src/ex_
    #11 0x55ec6e6b7a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
```

```
    #12 0x55ec6ecb3eda in exe_commands /home/fuzz/vim/src/main.c:3133
    #13 0x55ec6ecad048 in vim_main2 /home/fuzz/vim/src/main.c:780
    #14 0x55ec6ecac900 in main /home/fuzz/vim/src/main.c:432

    #15 0x7fa0c810e082 in __libc_start_main ../csu/libc-start.c:308
    #16 0x55ec6e538e4d in _start (/home/fuzz/vim/src/vim+0x139e4d)

0x602000006111 is located 0 bytes to the right of 1-byte region [0x60200000
allocated by thread T0 here:
    #0 0x7fa0c85a5808 in __interceptor_malloc ../../../../src/libsanitizer/
    #1 0x55ec6e53928a in lalloc /home/fuzz/vim/src/alloc.c:246
    #2 0x55ec6e53907b in alloc /home/fuzz/vim/src/alloc.c:151
    #3 0x55ec6ea6f52d in vim_strsave /home/fuzz/vim/src/strings.c:27
    #4 0x55ec6e633a55 in eval_for_line /home/fuzz/vim/src/eval.c:1781
    #5 0x55ec6e6f1c4d in ex_while /home/fuzz/vim/src/ex_eval.c:1295
    #6 0x55ec6e6c2443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #7 0x55ec6e6b96e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #8 0x55ec6e9dc845 in do_source_ext /home/fuzz/vim/src/scriptfile.c:1674
    #9 0x55ec6e9dd977 in do_source /home/fuzz/vim/src/scriptfile.c:1801
    #10 0x55ec6e9da506 in cmd_source /home/fuzz/vim/src/scriptfile.c:1174
    #11 0x55ec6e9da56b in ex_source /home/fuzz/vim/src/scriptfile.c:1200
    #12 0x55ec6e6c2443 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2570
    #13 0x55ec6e6b96e6 in do_cmdline /home/fuzz/vim/src/ex_docmd.c:992
    #14 0x55ec6e6b7a80 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:586
    #15 0x55ec6ecb3eda in exe_commands /home/fuzz/vim/src/main.c:3133
    #16 0x55ec6ecad048 in vim_main2 /home/fuzz/vim/src/main.c:780
    #17 0x55ec6ecac900 in main /home/fuzz/vim/src/main.c:432
    #18 0x7fa0c810e082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/vim/src/mbyte.c:
Shadow bytes around the buggy address:
  0x0c047fff8bd0: fa fa 06 fa fa fa fd fa fa fa fd fa fa fa 07 fa
  0x0c047fff8be0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8bf0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8c00: fa fa fd fa fa fa 00 00 fa fa 00 00 fa fa 05 fa
  0x0c047fff8c10: fa fa 00 00 fa fa fd fa fa fa fd fd fa fa 07 fa
=>0x0c047fff8c20: fa fa[01]fa fa fa fd fa fa fa 01 fa fa fa 06 fa
  0x0c047fff8c30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8c60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c04/fff8c70: 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
==66771==ABORTING
```

poc4_hbo.dat

Impact

This vulnerability is capable of crashing software, modify memory, and possible remote execution.

CVE
CVE-2022-2849
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity

High (7.8)

Registry
Other

Affected Version
<=v9.0.0213

Visibility
Public

Status
Fixed

Found by

janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 740 times.

We are processing your report and will contact the **vim** team within 24 hours. 3 months ago

We have contacted a member of the **vim** team and are waiting to hear back 3 months ago

Bram Moolenaar validated this vulnerability 3 months ago

I can reproduce it. The function to get the length works differently between latin and utf-8, that's bad.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 3 months ago Maintainer

Fixed with patch 9.0.0220

Bram Moolenaar marked this as fixed in 9.0.0219 with commit f6d39c 3 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation