NULL Pointer Dereference in function vim_regexec_string at regexp.c:2733 in vim/vim

1

✓ Valid Reported on May 9th 2022

Description

NULL Pointer Dereference in function vim_regexec_string at regexp.c:2733 allows attackers to cause a denial of service (application crash) via a crafted input.

vim version

```
git log
commit b370771bffc8395204f53209b69e35dff95a9237 (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -X -Z -e -s -S ./poc_n2_s.dat -c :qa!
Segmentation fault
```

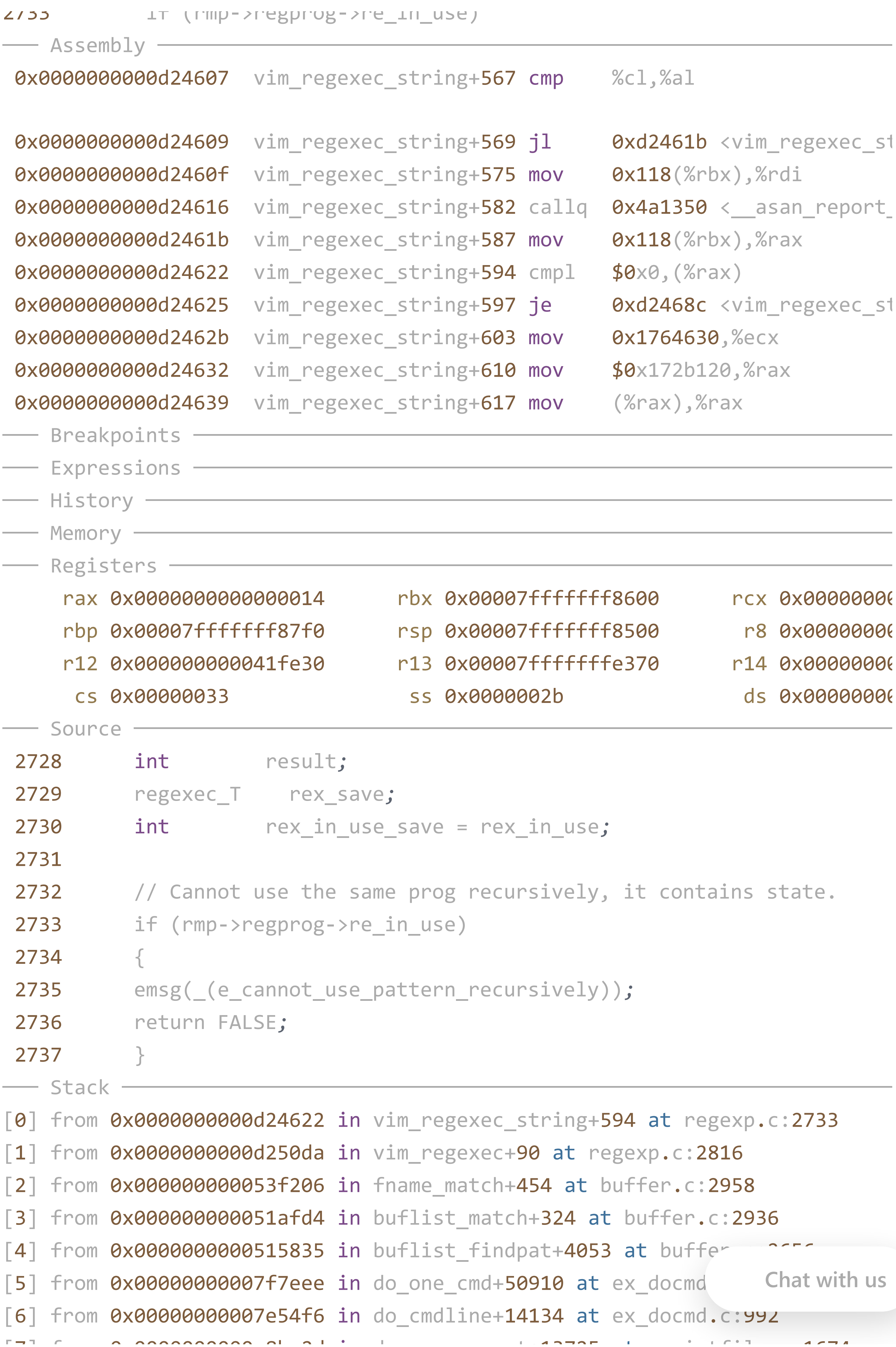
poc_n2_s.dat

GDB

```
── Output/messages ──────────────────────────────────────────
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x0000000000d24622 in vim_regexec_string (rmp=0x7fffffff8900, line=0x60600
2733            if (rmp->regprog->re_in_use)
```

Chat with us



```
2733        if (rmp->regprog->re_in_use)
─── Assembly ───────────────────────────────────────────────────────────────
 0x0000000000d24607  vim_regexec_string+567 cmp    %cl,%al

 0x0000000000d24609  vim_regexec_string+569 jl     0xd2461b <vim_regexec_st
 0x0000000000d2460f  vim_regexec_string+575 mov    0x118(%rbx),%rdi
 0x0000000000d24616  vim_regexec_string+582 callq  0x4a1350 <__asan_report_
 0x0000000000d2461b  vim_regexec_string+587 mov    0x118(%rbx),%rax
 0x0000000000d24622  vim_regexec_string+594 cmpl   $0x0,(%rax)
 0x0000000000d24625  vim_regexec_string+597 je     0xd2468c <vim_regexec_st
 0x0000000000d2462b  vim_regexec_string+603 mov    0x1764630,%ecx
 0x0000000000d24632  vim_regexec_string+610 mov    $0x172b120,%rax
 0x0000000000d24639  vim_regexec_string+617 mov    (%rax),%rax
─── Breakpoints ────────────────────────────────────────────────────────────
─── Expressions ────────────────────────────────────────────────────────────
─── History ────────────────────────────────────────────────────────────────
─── Memory ─────────────────────────────────────────────────────────────────
─── Registers ──────────────────────────────────────────────────────────────
    rax 0x0000000000000014      rbx 0x00007fffffff8600      rcx 0x00000000
    rbp 0x00007fffffff87f0      rsp 0x00007fffffff8500       r8 0x00000000
    r12 0x000000000041fe30      r13 0x00007fffffffe370      r14 0x00000000
     cs 0x00000033               ss 0x0000002b               ds 0x00000000
─── Source ─────────────────────────────────────────────────────────────────
 2728       int         result;
 2729       regexec_T     rex_save;
 2730       int         rex_in_use_save = rex_in_use;
 2731
 2732       // Cannot use the same prog recursively, it contains state.
 2733       if (rmp->regprog->re_in_use)
 2734       {
 2735       emsg(_(e_cannot_use_pattern_recursively));
 2736       return FALSE;
 2737       }
─── Stack ──────────────────────────────────────────────────────────────────
[0] from 0x0000000000d24622 in vim_regexec_string+594 at regexp.c:2733
[1] from 0x0000000000d250da in vim_regexec+90 at regexp.c:2816
[2] from 0x000000000053f206 in fname_match+454 at buffer.c:2958
[3] from 0x000000000051afd4 in buflist_match+324 at buffer.c:2936
[4] from 0x0000000000515835 in buflist_findpat+4053 at buffe
[5] from 0x00000000007f7eee in do_one_cmd+50910 at ex_docmd
[6] from 0x00000000007e54f6 in do_cmdline+14134 at ex_docmd.c:992
```

```
[7] from 0x000000000000e8be2d in do_source_ext+13725 at scriptfile.c:1674
[8] from 0x0000000000e88887 in do_source+103 at scriptfile.c:1801
[9] from 0x0000000000e881bd in cmd_source+2317 at scriptfile.c:1174

[+]
── Threads ──────────────────────────────────────────────────────────────────
[1] id 579181 name vim from 0x0000000000d24622 in vim_regexec_string+594 at
── Variables ────────────────────────────────────────────────────────────────
arg rmp = 0x7fffffff8900: {regprog = 0x0,startp = {[0] = 0x7fffffff8c88 "\(
loc result = -1, rex_save = {reg_match = 0x618000002f00,reg_mmatch = 0x100(
─────────────────────────────────────────────────────────────────────────────
>>> p rmp->regprog
$1 = (regprog_T *) 0x0
>>>
```

Impact

NULL Pointer Dereference in function vim_regexec_string at regexp.c:2733 allows attackers to cause a denial of service (application crash) via a crafted input.

CVE
CVE-2022-1674
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (6.6)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Chat with us

Found by
TDHX ICS Security

TDHX ICS Security

@jieyongma

pro

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 948 times.

We are processing your report and will contact the **vim** team within 24 hours. 7 months ago

We have contacted a member of the **vim** team and are waiting to hear back 7 months ago

Bram Moolenaar 7 months ago Maintainer

Very similar to what was fixed in 8.2.4901, but a different code path.

Bram Moolenaar validated this vulnerability 7 months ago

TDHX ICS Security has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 7 months ago Maintainer

Fixed in patch 8.2.4938

Bram Moolenaar marked this as fixed in **8.2** with commit **a59f2d** 7 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

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