Null pointer dereference in function diff_check in vim/vim

0

Valid Reported on Jun 24th 2022

Description

Null pointer dereference in function `diff_check` at diff.c:1923

Version

```
commit 8eba2bd291b347e3008aa9e565652d51ad638cfa (HEAD, tag: v8.2.5151)
```

Proof of Concept

```
guest@elk:~/trung/vim2/src$ valgrind ./vim -u NONE -i NONE -n -m -X -Z -e -
==4357== Memcheck, a memory error detector
==4357== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==4357== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright infc
==4357== Command: ./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/guest/tr
==4357==
  debug=  define=^\s*#\s*define  dictionary=  diffexpr=  diffopt=internal,f
==4357== Invalid read of size 8
==4357==    at 0x16CA0B: diff_check (diff.c:1923)
==4357==    by 0x16BE02: diff_redraw (diff.c:684)
==4357==    by 0x16C832: ex_diffupdate (diff.c:1001)
==4357==    by 0x16CA46: diff_check (diff.c:1917)
==4357==    by 0x16BE02: diff_redraw (diff.c:684)
==4357==    by 0x16BF9D: diff_buf_delete (diff.c:122)
==4357==    by 0x149DF3: buf_freeall (buffer.c:851)
==4357==    by 0x14B9C7: close_buffer (buffer.c:676)
==4357==    by 0x266C0C: wipe_qf_buffer (quickfix.c:1972)
==4357==    by 0x266C0C: ll_free_all (quickfix.c:2005)
==4357==    by 0x26B233: qf_free_all (quickfix.c:2025)
==4357==    by 0x34E7AF: win_free (window.c:5252)
```

```
==4357==    by 0x35108A: win_free_mem (window.c:2941)
==4357==  Address 0x0 is not stack'd, malloc'd or (recently) free'd
==4357==

==4357==
==4357== Process terminating with default action of signal 11 (SIGSEGV)
==4357==    at 0x5851177: kill (syscall-template.S:78)
==4357==    by 0x254A47: may_core_dump (os_unix.c:3448)
==4357==    by 0x254A47: mch_exit (os_unix.c:3484)
==4357==    by 0x37FD2A: getout (main.c:1737)
==4357==    by 0x5850F0F: ??? (in /lib/x86_64-linux-gnu/libc-2.27.so)
==4357==    by 0x16CA0A: diff_check (diff.c:1923)
==4357==    by 0x16BE02: diff_redraw (diff.c:684)
==4357==    by 0x16C832: ex_diffupdate (diff.c:1001)
==4357==    by 0x16CA46: diff_check (diff.c:1917)
==4357==    by 0x16BE02: diff_redraw (diff.c:684)
==4357==    by 0x16BF9D: diff_buf_delete (diff.c:122)
==4357==    by 0x149DF3: buf_freeall (buffer.c:851)
==4357==    by 0x14B9C7: close_buffer (buffer.c:676)
==4357==
==4357== HEAP SUMMARY:
==4357==     in use at exit: 424,339 bytes in 1,303 blocks
==4357==   total heap usage: 8,647 allocs, 7,344 frees, 5,819,314 bytes all
==4357==
==4357== LEAK SUMMARY:
==4357==    definitely lost: 18,224 bytes in 13 blocks
==4357==    indirectly lost: 0 bytes in 0 blocks
==4357==      possibly lost: 0 bytes in 0 blocks
==4357==    still reachable: 406,115 bytes in 1,290 blocks
==4357==         suppressed: 0 bytes in 0 blocks
==4357== Rerun with --leak-check=full to see details of leaked memory
==4357==
==4357== For counts of detected and suppressed errors, rerun with: -v
==4357== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
Segmentation fault
```

Attachment

poc22

Impact

DoS: Crash, Exit, or Restart

CVE
CVE-2022-2208
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
High (7.8)

Registry
Other

Affected Version
8.2.5151

Visibility
Public

Status
Fixed

Found by

xikhud
@acquykhud
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 620 times.

We are processing your report and will contact the vim team within 24 hour

We have contacted a member of the vim team and are waiting to hear back 5 months ago

Bram Moolenaar validated this vulnerability 5 months ago

I can reproduce it. I'll use a simplified version of the POC for a test.

xikhud has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 5 months ago Maintainer

Fixed with patch 8.2.5163

Bram Moolenaar marked this as fixed in 8.2 with commit cd38bb 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us