huntr

Null pointer dereference in function skipwhite in vim/vim

0

✓ Valid Reported on Jun 26th 2022

Description

Null pointer dereference in function `skipwhite` at charset.c:1428

Version

```
commit c101abff4c6756db4f5e740fde289decb9452efa (HEAD -> master, tag: v8.2.
```

Proof of Concept

```
guest@elk:~/trung$ valgrind ./vim_latest/src/vim -u NONE -i NONE -n -m -X -
==32519== Memcheck, a memory error detector
==32519== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==32519== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright inf
==32519== Command: ./vim_latest/src/vim -u NONE -i NONE -n -m -X -Z -e -s -
==32519==
==32519== Invalid read of size 1
==32519==    at 0x37B490: skipwhite (charset.c:1428)
==32519==    by 0x18AC60: eval0_retarg (eval.c:2391)
==32519==    by 0x1BDED8: ex_eval (ex_eval.c:951)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
```

```
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==  Address 0x0 is not stack'd, malloc'd or (recently) free'd
==32519==
==32519==
==32519== Process terminating with default action of signal 11 (SIGSEGV): c
==32519==    at 0x5851177: kill (syscall-template.S:78)
==32519==    by 0x254A97: may_core_dump (os_unix.c:3449)
==32519==    by 0x254A97: mch_exit (os_unix.c:3485)
==32519==    by 0x37FDAA: getout (main.c:1737)
==32519==    by 0x5850F0F: ??? (in /lib/x86_64-linux-gnu/libc-2.27.so)
==32519==    by 0x37B48F: ??? (charset.c:1418)
==32519==    by 0x18AC60: eval0_retarg (eval.c:2391)
==32519==    by 0x1BDED8: ex_eval (ex_eval.c:951)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==32519==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==32519==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==32519==
==32519== HEAP SUMMARY:
==32519==     in use at exit: 370,167 bytes in 2,757 blocks
==32519==   total heap usage: 4,952 allocs, 2,195 frees, 1,646,883 bytes al
==32519==
==32519== LEAK SUMMARY:
==32519==    definitely lost: 2,849 bytes in 3 blocks
==32519==    indirectly lost: 0 bytes in 0 blocks
==32519==      possibly lost: 0 bytes in 0 blocks
==32519==    still reachable: 367,318 bytes in 2,754 blocks
==32519==         suppressed: 0 bytes in 0 blocks
==32519== Rerun with --leak-check=full to see details of leaked memory
==32519==
==32519== For counts of detected and suppressed errors, rer
==32519== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

```
Segmentation fault
```

Attachment

poc40min

Impact

DoS: Crash, Exit, or Restart

CVE
CVE-2022-2231
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
High (7.8)

Registry
Other

Affected Version
8.2.5164

Visibility
Public

Status
Fixed

Found by

xikhud
@acquykhud
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 650 times.

We are processing your report and will contact the **vim** team within 24 hours. 5 months ago

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 the problem. I'll use the POC for a regression 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 8.2.5169

Bram Moolenaar marked this as fixed in **8.,2** with commit **794813** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation