Bug 14781 - A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function

Status: RESOLVED FIXED

Alias: None

Product: Busybox
Component: Standard Compliance (show other bugs)
Version: 1.35.x
Hardware: All Linux

Importance: P5 major
Target Milestone: ---
Assignee: unassigned

URL:
Keywords:

Depends on:
Blocks:

Reported: 2022-04-27 06:31 UTC by Taolaw
Modified: 2022-07-29 02:24 UTC (History)
CC List: 4 users (show)

See Also:
Host:
Build:

Attachments	
poc (24 bytes, application/octet-stream) 2022-04-27 06:31 UTC, Taolaw	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

Taolaw 2022-04-27 06:31:51 UTC Description

```
Created attachment 9301 [details]
poc

Discoverer: Taolaw@Vlab of Vecentek

command: ./busybox_unstripped awk -f crash2 1.txt

=================================================================
==716531==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000001d60 at
pc 0x55df2f6b595d bp 0x7fffc8cf08a0 sp 0x7fffc8cf0890
READ of size 4 at 0x606000001d60 thread T0
    #0 0x55df2f6b595c in copyvar editors/awk.c:1051

0x606000001d60 is located 0 bytes inside of 64-byte region
[0x606000001d60,0x606000001da0)
freed by thread T0 here:
    #0 0x7f7b1aeec40f in __interceptor_free
../../../../src/libsanitizer/asan/asan_malloc_linux.cc:122
```

```
    #1 0x55df2f6bf305 in nvfree editors/awk.c:1840
    #2 0x55df2f95bdff  (/home/test/fuzz/busybox-ASAN/busybox_unstripped+0x1044dff)

previously allocated by thread T0 here:
    #0 0x7f7b1aeec808 in __interceptor_malloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cc:144
    #1 0x55df2f1b24a5 in xmalloc libbb/xfuncs_printf.c:50
    #2 0x55df2f95bdff  (/home/test/fuzz/busybox-ASAN/busybox_unstripped+0x1044dff)

SUMMARY: AddressSanitizer: heap-use-after-free editors/awk.c:1051 in copyvar
Shadow bytes around the buggy address:
  0x0c0c7fff8350: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c7fff8360: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c7fff8370: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c0c7fff8380: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c7fff8390: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
=>0x0c0c7fff83a0: fd fd fd fd fd fd fd fd fa fa fa fa[fd]fd fd fd
  0x0c0c7fff83b0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c7fff83c0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c7fff83d0: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c0c7fff83e0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c7fff83f0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
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
==716531==ABORTING
```

Steve Beattie 2022-05-20 05:31:58 UTC Comment 1

This issue was assigned CVE-2022-30065 (https://nvd.nist.gov/vuln/detail/CVE-2022-30065).

Natanael Copa 2022-06-07 18:32:17 UTC Comment 2

I'm trying to reproduce this here. What is the content of `1.txt`?

Natanael Copa 2022-06-07 18:40:38 UTC Comment 3

It does not crash here but valgrind detects it and various other use after free:

```
$ echo foo | valgrind ./busybox_unstripped awk '$3i$3in$9=$r||$9=i6/6-9f'
==3430== Memcheck, a memory error detector
==3430== Copyright (C) 2002-2022, and GNU GPL'd, by Julian Seward et al.
==3430== Using Valgrind-3.19.0 and LibVEX; rerun with -h for copyright info
==3430== Command: ./busybox_unstripped awk $3i$3in$9=$r||$9=i6/6-9f
```

```
==3430==
==3430== Invalid read of size 4
==3430==    at 0x195B74: copyvar (awk.c:1064)
==3430==    by 0x196ED1: evaluate (awk.c:3141)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b7510 is 0 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x19698C: evaluate (awk.c:2923)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x19698C: evaluate (awk.c:2923)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 8
==3430==    at 0x195B76: copyvar (awk.c:1066)
==3430==    by 0x196ED1: evaluate (awk.c:3141)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b7520 is 16 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x19698C: evaluate (awk.c:2923)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
```

```
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x19698C: evaluate (awk.c:2923)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 8
==3430==    at 0x195B7B: copyvar (awk.c:1067)
==3430==    by 0x196ED1: evaluate (awk.c:3141)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b7518 is 8 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x19698C: evaluate (awk.c:2923)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x19698C: evaluate (awk.c:2923)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 4
==3430==    at 0x1947E6: getvar_i (awk.c:1023)
==3430==    by 0x194869: is_numeric (awk.c:1082)
==3430==    by 0x194869: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
```

```
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c10 is 0 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid write of size 8
==3430==    at 0x1947EF: getvar_i (awk.c:1024)
==3430==    by 0x194869: is_numeric (awk.c:1082)
==3430==    by 0x194869: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c20 is 16 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
```

```
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 8
==3430==    at 0x1947F7: getvar_i (awk.c:1025)
==3430==    by 0x194869: is_numeric (awk.c:1082)
==3430==    by 0x194869: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c18 is 8 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid write of size 4
==3430==    at 0x194839: getvar_i (awk.c:1039)
==3430==    by 0x194869: is_numeric (awk.c:1082)
==3430==    by 0x194869: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c10 is 0 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
```

```
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 4
==3430==    at 0x19483B: getvar_i (awk.c:1041)
==3430==    by 0x194869: is_numeric (awk.c:1082)
==3430==    by 0x194869: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c10 is 0 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 8
==3430==    at 0x194841: getvar_i (awk.c:1044)
==3430==    by 0x194869: is_numeric (awk.c:1082)
==3430==    by 0x194869: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
```

```
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c20 is 16 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 4
==3430==    at 0x19486A: is_numeric (awk.c:1083)
==3430==    by 0x19486A: istrue (awk.c:1089)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c10 is 0 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
```

```
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430== Invalid read of size 8
==3430==    at 0x19488D: istrue (awk.c:1091)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Address 0x48b6c18 is 8 bytes inside a block of size 64 free'd
==3430==    at 0x48A4B0D: free (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-
linux.so)
==3430==    by 0x1974EA: evaluate (awk.c:3537)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==  Block was alloc'd at
==3430==    at 0x48A26D5: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-
amd64-linux.so)
==3430==    by 0x117287: xmalloc (xfuncs_printf.c:50)
==3430==    by 0x1172BC: xzalloc (xfuncs_printf.c:71)
==3430==    by 0x1968F6: nvalloc (awk.c:1825)
==3430==    by 0x1968F6: evaluate (awk.c:2877)
==3430==    by 0x1983EB: ptest (awk.c:2227)
==3430==    by 0x196A25: evaluate (awk.c:2951)
==3430==    by 0x19885A: awk_main (awk.c:3713)
==3430==    by 0x11600D: run_applet_no_and_exit (appletlib.c:967)
==3430==    by 0x116331: run_applet_and_exit (appletlib.c:986)
==3430==    by 0x116314: busybox_main (appletlib.c:917)
==3430==    by 0x116314: run_applet_and_exit (appletlib.c:979)
==3430==    by 0x1163AA: main (appletlib.c:1126)
==3430==
==3430==
==3430== HEAP SUMMARY:
==3430==     in use at exit: 11,033 bytes in 174 blocks
==3430==   total heap usage: 204 allocs, 30 frees, 13,028 bytes allocated
==3430==
==3430== LEAK SUMMARY:
==3430==    definitely lost: 0 bytes in 0 blocks
==3430==    indirectly lost: 0 bytes in 0 blocks
==3430==      possibly lost: 11,033 bytes in 174 blocks
==3430==    still reachable: 0 bytes in 0 blocks
==3430==         suppressed: 0 bytes in 0 blocks
==3430== Rerun with --leak-check=full to see details of leaked memory
==3430==
==3430== For lists of detected and suppressed errors, rerun with: -s
==3430== ERROR SUMMARY: 12 errors from 11 contexts (suppressed: 0 from 0)
```

Natanael Copa 2022-06-07 18:49:18 UTC Comment 4

```
simpler way to reproduce it:

echo "foo" | valgrind ./busybox_unstripped awk '$1$1=0'
```

Natanael Copa 2022-06-07 19:14:25 UTC Comment 5

This change makes it segfault early:

```
$ git diff
diff --git a/editors/awk.c b/editors/awk.c
index 079d0bde5..840f2595f 100644
--- a/editors/awk.c
+++ b/editors/awk.c
@@ -55,7 +55,7 @@
 /* If you comment out one of these below, it will be #defined later
  * to perform debug printfs to stderr: */
 #define debug_printf_walker(...)  do {} while (0)
-#define debug_printf_eval(...)  do {} while (0)
+//#define debug_printf_eval(...)  do {} while (0)
 #define debug_printf_parse(...)  do {} while (0)

 #ifndef debug_printf_walker
@@ -2922,7 +2922,7 @@ static var *evaluate(node *op, var *res)
                if (opinfo & OF_RES2) {
                        R.v = evaluate(op->r.n, TMPVAR1);
                        //TODO: L.v may be invalid now, set L.v to NULL to catch
bugs?
-                       //L.v = NULL;
+                       L.v = NULL;
                        if (opinfo & OF_STR2) {
                                R.s = getvar_s(R.v);
                                debug_printf_eval("R.s:'%s'\n", R.s);
$ echo "foo" | ./busybox_unstripped awk '$1$1=0'
fsrealloc: xrealloc(0, 512)
fsrealloc: Fields=0x7f6dbda05030..0x7f6dbda0522f
getvar_i: 0.000000
getvar_i: 1.000000
entered awk_getline()
returning from awk_getline(): 1
getvar_i: 0.000000
getvar_i: 0.000000
entered evaluate()
opinfo:00000300 opn:00000000
switch(0x3)
NEWSOURCE
opinfo:00000d00 opn:00000000
switch(0xd)
TEST
entered evaluate()
opinfo:4a031f00 opn:00000000
entered evaluate()
opinfo:230f1500 opn:00000000
entered evaluate()
opinfo:05021700 opn:00000000
entered evaluate()
opinfo:00002700 opn:00000000
switch(0x27)
VAR
returning from evaluate(): 0x7f6dbda03410
switch(0x17)
FIELD
getvar_i: 1.000000
returning from evaluate(): 0x7f6dbda05030
L.s:'foo'
entered evaluate()
opinfo:05021700 opn:00000000
entered evaluate()
opinfo:00002700 opn:00000000
switch(0x27)
```

```
VAR
returning from evaluate(): 0x7f6dbda034d0
switch(0x17)
FIELD
getvar_i: 1.000000
returning from evaluate(): 0x7f6dbda05030
R.s:'foo'
switch(0x15)
CONCAT /
COMMA
returning from evaluate(): 0x7f6dbda04bb0
entered evaluate()
opinfo:00002700 opn:00000000
switch(0x27)
VAR
returning from evaluate(): 0x7f6dbda03560
switch(0x1f)
MOVE
Segmentation fault
```

Natanael Copa 2022-06-07 19:31:09 UTC Comment 6

Possible fix:

```
diff --git a/editors/awk.c b/editors/awk.c
index 079d0bde5..d68b8d4bc 100644
--- a/editors/awk.c
+++ b/editors/awk.c
@@ -2922,7 +2922,7 @@ static var *evaluate(node *op, var *res)
                if (opinfo & OF_RES2) {
                        R.v = evaluate(op->r.n, TMPVAR1);
                        //TODO: L.v may be invalid now, set L.v to NULL to catch
bugs?
-                       //L.v = NULL;
+                       L.v = NULL;
                        if (opinfo & OF_STR2) {
                                R.s = getvar_s(R.v);
                                debug_printf_eval("R.s:'%s'\n", R.s);
@@ -3128,6 +3128,8 @@ static var *evaluate(node *op, var *res)

                case XC( OC_MOVE ):
                        debug_printf_eval("MOVE\n");
+                       if (L.v == NULL)
+                               syntax_error(EMSG_POSSIBLE_ERROR);
                        /* if source is a temporary string, jusk relink it to dest
*/
                        if (R.v == TMPVAR1
                         && !(R.v->type & VF_NUMBER)
```

Natanael Copa 2022-06-17 09:49:42 UTC Comment 7

(In reply to Natanael Copa from comment #6)

Setting L.v to null does not work. it breaks other stuff.

This might work and ./runtests awk passes:

```
diff --git a/editors/awk.c b/editors/awk.c
index 079d0bde5..acdc50e32 100644
--- a/editors/awk.c
+++ b/editors/awk.c
@@ -3128,6 +3128,9 @@ static var *evaluate(node *op, var *res)
```

```
                case XC( OC_MOVE ):
                        debug_printf_eval("MOVE\n");
+                       /* make sure that we never return a temp var */
+                       if (L.v == TMPVAR0)
+                               L.v = res;
                        /* if source is a temporary string, jusk relink it to dest
*/
                        if (R.v == TMPVAR1)
                         && !(R.v->type & VF_NUMBER)
```

Denys Vlasenko 2022-07-11 23:30:06 UTC Comment 8

Fixed in git

xiechengliang 2022-07-29 02:24:00 UTC Comment 9

Does the vulnerability affect versions 1.32.1 and 1.34.1?