Bug 701799 - global-buffer-overflow at contrib/japanese/gdevmjc.c:1509 in mj_color_correct

Status: RESOLVED FIXED
Alias: None
Product: Ghostscript
Component: General (show other bugs)
Version: master
Hardware: PC Linux
Importance: P4 normal
Assignee: Julian Smith
URL:
Keywords:
Depends on:
Blocks:

Reported: 2019-10-26 15:06 UTC by Suhwan
Modified: 2019-10-30 09:51 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (25.73 KB, application/pdf) 2019-10-26 15:06 UTC, Suhwan	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.

Suhwan 2019-10-26 15:06:25 UTC Description

```
Created attachment 18382 [details]
poc

Hello.

I found a global-buffer-overflow bug in GhostScript.
Please confirm.
Thanks.


OS:        Ubuntu 18.04 64bit
Version:   commit bfeff28bb56ee4424ac78619792c18bf4f5104ef

Steps to reproduce:
1. Download the .POC files.
2. Compile the source code with "make sanitize" using gcc.
3. Run following cmd.


Here's ASAN report.

GPL Ghostscript GIT PRERELEASE 9.51 (2019-10-15)
Copyright (C) 2019 Artifex Software, Inc.  All rights reserved.
This software is supplied under the GNU AGPLv3 and comes with NO WARRANTY:
see the file COPYING for details.
   **** Error: invalid token after startxref.
              Output may be incorrect.
   **** Error:  An error occurred while reading an XREF table.
   **** The file has been damaged.  This may have been caused
   **** by a problem while converting or transfering the file.
   **** Ghostscript will attempt to recover the data.
   **** However, the output may be incorrect.
Processing pages 1 through 1.
Page 1
=================================================================
==685==ERROR: AddressSanitizer: global-buffer-overflow on address 0x563addc51380 at
pc 0x563adbdc62fa bp 0x7ffff2f7c830 sp 0x7ffff2f7c820
READ of size 2 at 0x563addc51380 thread T0
    #0 0x563adbdc62f9 in mj_color_correct contrib/japanese/gdevmjc.c:1509
    #1 0x563adbdc6c4d in gdev_mjc_map_rgb_color contrib/japanese/gdevmjc.c:1578
    #2 0x563adbdc7855 in gdev_mjc_encode_color contrib/japanese/gdevmjc.c:1658
    #3 0x563adc36a7f1 in gx_forward_encode_color base/gdevnfwd.c:810
    #4 0x563adc36a7f1 in gx_forward_encode_color base/gdevnfwd.c:810
    #5 0x563adc24aa7d in cmapper_vanilla base/gxcmap.c:2277
    #6 0x563adc3d326d in template_mem_transform_pixel_region_render_portrait
base/gdevdrop.c:1090
    #7 0x563adc3d393d in mem_transform_pixel_region_render_portrait_4
base/gdevdrop.c:1149
    #8 0x563adc3d3aa1 in mem_transform_pixel_region_render_portrait
base/gdevdrop.c:1167
    #9 0x563adc3d6aca in mem_transform_pixel_region_process_data
base/gdevdrop.c:1825
    #10 0x563adc3d76e9 in mem_transform_pixel_region base/gdevdrop.c:1889
    #11 0x563adc234988 in clip_transform_pixel_region base/gxclip.c:1627
    #12 0x563adb2f53b8 in image_render_color_icc_tpr base/gxicolor.c:1078
    #13 0x563adc29f16c in gx_image1_plane_data base/gxidata.c:237
    #14 0x563adc2a7827 in gx_image_plane_data_rows base/gximage.c:183
    #15 0x563adc2a7761 in gx_image_plane_data base/gximage.c:175
    #16 0x563adb895c91 in clist_playback_band base/gxclrast.c:1541
    #17 0x563adb8b56d8 in clist_playback_file_bands base/gxclread.c:920
    #18 0x563adb8b4eb5 in clist_render_rectangle base/gxclread.c:854
    #19 0x563adb8b3e8b in clist_rasterize_lines base/gxclread.c:743
    #20 0x563adb8b2c9a in clist_get_bits_rectangle base/gxclread.c:632
    #21 0x563adb91b9f5 in clist_get_bits_rect_mt base/gxclthrd.c:845
    #22 0x563adc3608ee in gx_default_get_bits base/gdevdgbr.c:54
    #23 0x563adb83c2a4 in gdev_prn_get_bits base/gdevprn.c:1687
    #24 0x563adb83c4fe in gdev_prn_copy_scan_lines base/gdevprn.c:1712
    #25 0x563adbdc371a in mj_print_page contrib/japanese/gdevmjc.c:1216
    #26 0x563adbdc1f32 in mj6000c_print_page contrib/japanese/gdevmjc.c:950
    #27 0x563adb8390ed in gx_default_print_page_copies base/gdevprn.c:1231
    #28 0x563adb838abc in gdev_prn_output_page_aux base/gdevprn.c:1133
    #29 0x563adb838d54 in gdev_prn_output_page base/gdevprn.c:1169
    #30 0x563adbf15f4c in gs_output_page base/gsdevice.c:212
    #31 0x563adc5754f5 in zoutputpage psi/zdevice.c:416
    #32 0x563adc492261 in do_call_operator psi/interp.c:86
    #33 0x563adc49b9e0 in interp psi/interp.c:1300
    #34 0x563adc493dae in gs_call_interp psi/interp.c:520
    #35 0x563adc493453 in gs_interpret psi/interp.c:477
    #36 0x563adc4679aa in gs_main_interpret psi/imain.c:253
    #37 0x563adc46ae5f in gs_main_run_string_end psi/imain.c:791
    #38 0x563adc46a824 in gs_main_run_string_with_length psi/imain.c:735
    #39 0x563adc46a796 in gs_main_run_string psi/imain.c:716
    #40 0x563adc47745a in run_string psi/imainarg.c:1117
    #41 0x563adc4771fd in runarg psi/imainarg.c:1086
    #42 0x563adc476a7c in argproc psi/imainarg.c:1008
    #43 0x563adc471248 in gs_main_init_with_args01 psi/imainarg.c:241
    #44 0x563adc4716ac in gs_main_init_with_args psi/imainarg.c:288
    #45 0x563adc47cbdc in psapi_init_with_args psi/psapi.c:272
    #46 0x563adc64c1fb in gsapi_init_with_args psi/iapi.c:148
    #47 0x563adb21d808 in main psi/gs.c:95
    #48 0x7ff2ddaccb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #49 0x563adb21d5a9 in _start (gs+0x36b5a9)

0x563addc51380 is located 0 bytes to the right of global variable 'grnsep2' defined
```

```
in './contrib/japanese/gdevmjc.h:2741:23' (0x563addc50f80) of size 1024
0x563addc51380 is located 32 bytes to the left of global variable 'esp_dat_c'
defined in './contrib/japanese/gdevmjc.h:2807:14' (0x563addc513a0) of size 2048
SUMMARY: AddressSanitizer: global-buffer-overflow contrib/japanese/gdevmjc.c:1509
in mj_color_correct
Shadow bytes around the buggy address:
  0x0ac7dbb82220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb82230: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb82240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb82250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb82260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ac7dbb82270:[f9]f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb82280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb82290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb822a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb822b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac7dbb822c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==685==ABORTING
```

Suhwan 2019-10-26 15:07:48 UTC **Comment 1**

```
please run following cmd:
gs -sOutputFile=tmp -sDEVICE=mj6000c $PoC
```

Julian Smith 2019-10-30 09:51:41 UTC **Comment 2**

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=849e74e5ab450dd581942192da7101e0664fa5af