Bug 701800 - heap-buffer-overflow at contrib/gdevbjca.c:758 in FloydSteinbergDitheringC

Status:	RESOLVED FIXED	**Reported:**	2019-10-26 15:11 UTC by Suhwan
		Modified:	2019-10-31 11:22 UTC (History)
Alias:	None	**CC List:**	0 users
Product:	Ghostscript		
Component:	General (show other bugs)	**See Also:**	
Version:	master	**Customer:**	
Hardware:	PC Linux	**Word Size:**	---
Importance:	P4 normal		
Assignee:	Julian Smith		
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments	
poc (25.73 KB, application/pdf) 2019-10-26 15:11 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 15:11:22 UTC Description

```
Created attachment 18383 [details]
poc

Hello.

I found a heap-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.

gs -sPAPERSIZE=legal -sOutputFile=tmp -sDEVICE=bjccolor $PoC

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.
Processing pages 1 through 1.
Page 1
=================================================================
==32948==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62b000006a7c at
pc 0x55a5fda282cf bp 0x7fff6a604110 sp 0x7fff6a604100
READ of size 4 at 0x62b000006a7c thread T0
    #0 0x55a5fda282ce in FloydSteinbergDitheringC contrib/gdevbjca.c:758
    #1 0x55a5fda2385a in bjc_print_page_color contrib/gdevbjc_.c:894
    #2 0x55a5fd5550ed in gx_default_print_page_copies base/gdevprn.c:1231
    #3 0x55a5fd554abc in gdev_prn_output_page_aux base/gdevprn.c:1133
    #4 0x55a5fd554d54 in gdev_prn_output_page base/gdevprn.c:1169
    #5 0x55a5fdc31f4c in gs_output_page base/gsdevice.c:212
    #6 0x55a5fe2914f5 in zoutputpage psi/zdevice.c:416
    #7 0x55a5fe1ae261 in do_call_operator psi/interp.c:86
    #8 0x55a5fe1b79e0 in interp psi/interp.c:1300
    #9 0x55a5fe1afdae in gs_call_interp psi/interp.c:520
    #10 0x55a5fe1af453 in gs_interpret psi/interp.c:477
    #11 0x55a5fe1839aa in gs_main_interpret psi/imain.c:253
    #12 0x55a5fe186e5f in gs_main_run_string_end psi/imain.c:791
    #13 0x55a5fe186824 in gs_main_run_string_with_length psi/imain.c:735
    #14 0x55a5fe186796 in gs_main_run_string psi/imain.c:716
    #15 0x55a5fe19345a in run_string psi/imainarg.c:1117
    #16 0x55a5fe1931fd in runarg psi/imainarg.c:1086
    #17 0x55a5fe192a7c in argproc psi/imainarg.c:1008
    #18 0x55a5fe18d248 in gs_main_init_with_args01 psi/imainarg.c:241
    #19 0x55a5fe18d6ac in gs_main_init_with_args psi/imainarg.c:288
    #20 0x55a5fe198bdc in psapi_init_with_args psi/psapi.c:272
    #21 0x55a5fe3681fb in gsapi_init_with_args psi/iapi.c:148
    #22 0x55a5fcf39808 in main psi/gs.c:95
    #23 0x7fdea0d52b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #24 0x55a5fcf395a9 in _start (gs+0x36b5a9)

0x62b000006a7c is located 460 bytes to the right of 26288-byte region
[0x62b000000200,0x62b0000068b0)
allocated by thread T0 here:
    #0 0x7fdea263cb50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x55a5fdc979a5 in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x55a5fdc072fa in alloc_acquire_clump base/gsalloc.c:2485
    #3 0x55a5fdc045a1 in alloc_obj base/gsalloc.c:1948
    #4 0x55a5fdbffcb9 in i_alloc_struct_immovable base/gsalloc.c:1255
    #5 0x55a5fdc33415 in gs_copydevice2 base/gsdevice.c:401
    #6 0x55a5fe28da46 in zcopydevice2 psi/zdevice.c:53
    #7 0x55a5fe1ae261 in do_call_operator psi/interp.c:86
    #8 0x55a5fe1b79e0 in interp psi/interp.c:1300
    #9 0x55a5fe1afdae in gs_call_interp psi/interp.c:520
    #10 0x55a5fe1af453 in gs_interpret psi/interp.c:477
    #11 0x55a5fe1839aa in gs_main_interpret psi/imain.c:253
    #12 0x55a5fe1866be in gs_run_init_file psi/imain.c:707
    #13 0x55a5fe183f5b in gs_main_init2aux psi/imain.c:301
    #14 0x55a5fe1841ff in gs_main_init2 psi/imain.c:338
    #15 0x55a5fe19305b in runarg psi/imainarg.c:1072
    #16 0x55a5fe192a7c in argproc psi/imainarg.c:1008
    #17 0x55a5fe18d248 in gs_main_init_with_args01 psi/imainarg.c:241
    #18 0x55a5fe18d6ac in gs_main_init_with_args psi/imainarg.c:288
    #19 0x55a5fe198bdc in psapi_init_with_args psi/psapi.c:272
    #20 0x55a5fe3681fb in gsapi_init_with_args psi/iapi.c:148
    #21 0x55a5fcf39808 in main psi/gs.c:95
    #22 0x7fdea0d52b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow contrib/gdevbjca.c:758 in
FloydSteinbergDitheringC
Shadow bytes around the buggy address:
  0x0c567fff8cf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c567fff8d00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c567fff8d10: 00 00 00 00 00 00 fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8d20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
=>0x0c567fff8d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]
  0x0c567fff8d50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8d60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8d70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8d80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c567fff8d90: fa fa fa fa fa fa fa fa fa fa fa fa 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
==32948==ABORTING
```

Julian Smith   2019-10-31 11:22:24 UTC   **Comment 1**

Fixed in https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=bf72f1a3dd5392ee8291e3b1518a0c2c5dc6ba39

Format For Printing - XML - Clone This Bug - Top of page