Bug 701801 - Division by Zero at contrib/japanese/gdev10v.c:288 in bj10v_print_page

Status:	RESOLVED FIXED	**Reported:**	2019-10-26 15:22 UTC by Suhwan
		Modified:	2022-10-17 07:18 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 15:22 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 15:22:05 UTC **Description**

```
Created attachment 18384 [details]
poc

Hello.

I found a division by zero 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 -dNOPAUSE -r169 -sOutputFile=tmp -sDEVICE=bj10v $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
ASAN:DEADLYSIGNAL
=================================================================
==42024==ERROR: AddressSanitizer: FPE on unknown address 0x5578729149e6 (pc
0x5578729149e6 bp 0x7ffce90caea0 sp 0x7ffce90cade0 T0)
    #0 0x5578729149e5 in bj10v_print_page contrib/japanese/gdev10v.c:288
    #1 0x5578724710ed in gx_default_print_page_copies base/gdevprn.c:1231
    #2 0x557872470abc in gdev_prn_output_page_aux base/gdevprn.c:1133
    #3 0x557872470d54 in gdev_prn_output_page base/gdevprn.c:1169
    #4 0x557872b4df4c in gs_output_page base/gsdevice.c:212
    #5 0x5578731ad4f5 in zoutputpage psi/zdevice.c:416
    #6 0x5578730ca261 in do_call_operator psi/interp.c:86
    #7 0x5578730d39e0 in interp psi/interp.c:1300
    #8 0x5578730cbdae in gs_call_interp psi/interp.c:520
    #9 0x5578730cb453 in gs_interpret psi/interp.c:477
    #10 0x55787309f9aa in gs_main_interpret psi/imain.c:253
    #11 0x5578730a2e5f in gs_main_run_string_end psi/imain.c:791
    #12 0x5578730a2824 in gs_main_run_string_with_length psi/imain.c:735
    #13 0x5578730a2796 in gs_main_run_string psi/imain.c:716
    #14 0x5578730af45a in run_string psi/imainarg.c:1117
    #15 0x5578730af1fd in runarg psi/imainarg.c:1086
    #16 0x5578730aea7c in argproc psi/imainarg.c:1008
    #17 0x5578730a9248 in gs_main_init_with_args01 psi/imainarg.c:241
    #18 0x5578730a96ac in gs_main_init_with_args psi/imainarg.c:288
    #19 0x5578730b4bdc in psapi_init_with_args psi/psapi.c:272
    #20 0x5578732841fb in gsapi_init_with_args psi/iapi.c:148
    #21 0x557871e55808 in main psi/gs.c:95
    #22 0x7f944547cb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #23 0x557871e555a9 in _start (gs+0x36b5a9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE contrib/japanese/gdev10v.c:288 in bj10v_print_page
==42024==ABORTING
```

Julian Smith 2019-10-31 11:27:15 UTC **Comment 1**

Fixed in https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=4fcbece46870

Ken Sharp 2022-10-17 07:18:09 UTC **Comment 3**

Spam comment marked private, user disabled.

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