Bug 701828 - Division by Zero at devices/gdevdm24.c:185 in dot24_print_page

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: 2019-11-02 15:19 UTC by Suhwan
Modified: 2019-11-04 15:52 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (25.73 KB, application/pdf) 2019-11-02 15:19 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 2019-11-02 15:19:19 UTC — Description

Created attachment 18419 [details]
poc

Hello

I found a Division by Zero bug in GhostScript.
Please confirm.
Thanks.

OS: Ubuntu 18.04 64bit
Version: commit 366ad48d076c1aa4c8f83c65011258a04e348207

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

```
gs -dBATCH -dNOPAUSE -dSAFER -r2 -sOutputFile=tmp -sDEVICE=necp6 $PoC
```

Here's ASAN report.

```
==27467==ERROR: AddressSanitizer: FPE on unknown address 0x55e310155c1a (pc
0x55e310155c1a bp 0x7fff025a67b0 sp 0x7fff025a6700 T0)
    #0 0x55e310155c19 in dot24_print_page devices/gdevdm24.c:185
    #1 0x55e310156778 in necp6_print_page devices/gdevdm24.c:271
    #2 0x55e30fbea302 in gx_default_print_page_copies base/gdevprn.c:1231
    #3 0x55e30fbe9cd1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #4 0x55e30fbe9fcb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #5 0x55e3102c7a25 in gs_output_page base/gsdevice.c:212
    #6 0x55e310926fce in zoutputpage psi/zdevice.c:416
    #7 0x55e310843d3a in do_call_operator psi/interp.c:86
    #8 0x55e31084d4b9 in interp psi/interp.c:1300
    #9 0x55e310845887 in gs_call_interp psi/interp.c:520
    #10 0x55e310844f2c in gs_interpret psi/interp.c:477
    #11 0x55e310819483 in gs_main_interpret psi/imain.c:253
    #12 0x55e31081c938 in gs_main_run_string_end psi/imain.c:791
    #13 0x55e31081c2fd in gs_main_run_string_with_length psi/imain.c:735
    #14 0x55e31081c26f in gs_main_run_string psi/imain.c:716
    #15 0x55e310828f33 in run_string psi/imainarg.c:1117
    #16 0x55e310828cd6 in runarg psi/imainarg.c:1086
    #17 0x55e310828555 in argproc psi/imainarg.c:1008
    #18 0x55e310822d21 in gs_main_init_with_args01 psi/imainarg.c:241
    #19 0x55e310823185 in gs_main_init_with_args psi/imainarg.c:288
    #20 0x55e31082e6b5 in psapi_init_with_args psi/psapi.c:272
    #21 0x55e3109fdcd4 in gsapi_init_with_args psi/iapi.c:148
    #22 0x55e30f5ce7f8 in main psi/gs.c:95
    #23 0x7f25f9f56b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #24 0x55e30f5ce599 in _start (gs+0x36c599)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE devices/gdevdm24.c:185 in dot24_print_page
```

Ken Sharp 2019-11-02 15:31:47 UTC — Comment 1

The divisor is 'bytes_per_space' which is calculated as 'dots_per_space * 3'. The variable dots_per_space is 'xres / 10'. So when xres is less than 3 bytes_per_space becomes 0.

Again this looks like the device is a fixed 360 dpi device, so we should throw a rangecheck on attempts to change the resolution. Its possible the device can accept mulitples of 360 (eg 12, 240 etc) but certainly we should not accept resolutions less than 3. Given these are dot matrix devices I'd be inclined to just freeze the resolution and wait to see if anyone complains.

Julian Smith 2019-11-04 15:52:41 UTC — Comment 2

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=eaba1d97b62831b42c51840cc8ee2bc4576c942e