Bug 701815 - global-buffer-overflow at devices/gdev3852.c:122 in jetp3852_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:	2019-10-31 17:59 UTC by Suhwan
Modified:	2019-11-01 18:30 UTC (History)
CC List:	0 users
See Also:	
Customer:	
Word Size:	---

Attachments	
poc (4.51 MB, application/pdf) 2019-10-31 17:59 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 2019-10-31 17:59:16 UTC **Description**

Created attachment 18399 [details]
poc

Hello

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

```
OS:        Ubuntu 18.04 64bit
Version:   commit b5bc53eb7223f8999882a5d8e2e35c27fe7a0b57
```

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 -sOutputFile=tmp -sDEVICE=jetp3852 $PoC
```

Here's ASAN report.

```
==34797==ERROR: AddressSanitizer: global-buffer-overflow on address 0x559fdeca84d0
at pc 0x559fdce3cd8c bp 0x7ffc43e989a0 sp 0x7ffc43e98990
READ of size 8 at 0x559fdeca84d0 thread T0
    #0 0x559fdce3cd8b in jetp3852_print_page devices/gdev3852.c:122
    #1 0x559fdc8f3ac5 in gx_default_print_page_copies base/gdevprn.c:1231
    #2 0x559fdc8f3494 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #3 0x559fdc8f378e in gdev_prn_bg_output_page base/gdevprn.c:1181
    #4 0x559fdcfd0dcd in gs_output_page base/gsdevice.c:212
    #5 0x559fdd630376 in zoutputpage psi/zdevice.c:416
    #6 0x559fdd54d0e2 in do_call_operator psi/interp.c:86
    #7 0x559fdd556861 in interp psi/interp.c:1300
    #8 0x559fdd54ec2f in gs_call_interp psi/interp.c:520
    #9 0x559fdd54e2d4 in gs_interpret psi/interp.c:477
    #10 0x559fdd52282b in gs_main_interpret psi/imain.c:253
    #11 0x559fdd525ce0 in gs_main_run_string_end psi/imain.c:791
    #12 0x559fdd5256a5 in gs_main_run_string_with_length psi/imain.c:735
    #13 0x559fdd525617 in gs_main_run_string psi/imain.c:716
    #14 0x559fdd5322db in run_string psi/imainarg.c:1117
    #15 0x559fdd53207e in runarg psi/imainarg.c:1086
    #16 0x559fdd5318fd in argproc psi/imainarg.c:1008
    #17 0x559fdd52c0c9 in gs_main_init_with_args01 psi/imainarg.c:241
    #18 0x559fdd52c52d in gs_main_init_with_args psi/imainarg.c:288
    #19 0x559fdd537a5d in psapi_init_with_args psi/psapi.c:272
    #20 0x559fdd70707c in gsapi_init_with_args psi/iapi.c:148
    #21 0x559fdc2d81d8 in main psi/gs.c:95
    #22 0x7feb135f8b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #23 0x559fdc2d7f79 in _start (gs+0x36bf79)

0x559fdeca84d0 is located 0 bytes to the right of global variable 'jetp3852_procs'
defined in './devices/gdev3852.c:45:24' (0x559fdeca8280) of size 592
SUMMARY: AddressSanitizer: global-buffer-overflow devices/gdev3852.c:122 in
jetp3852_print_page
Shadow bytes around the buggy address:
  0x0ab47bd8d040: f9 f9 f9 f9 00 00 00 00 00 00 00 00 f9 f9 f9 f9
  0x0ab47bd8d050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ab47bd8d090: 00 00 00 00 00 00 00 00 00 00[f9]f9 f9 f9 f9 f9
  0x0ab47bd8d0a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d0b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d0c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab47bd8d0e0: 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
```

Julian Smith 2019-11-01 18:30:55 UTC **Comment 1**

Fixed in: https://git.ghostscript.com/?
p=ghostpdl.git;a=commit;h=366ad48d076c1aa4c8f83c65011258a04e348207

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