Bug 701794 - global-buffer-overflow at devices/gdevepsc.c:186 in epsc_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: 2019-10-26 06:30 UTC by Suhwan
Modified: 2019-10-30 09:50 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (7.17 KB, application/pdf) 2019-10-26 06:30 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 06:30:53 UTC — Description

Created attachment 18378 [details]
poc

Hello.

I found a global-buffer-overflow bug in GhostScript.

Please confirm.

Thanks.

OS: Ubuntu 18.04 64bit

Steps to reproduce:
1. Download the .POC files.
2. Compile the source code with ASan.
3. Run following cmd.

```
gs -r680 -sOutputFile=tmp -sDEVICE=epsonc $PoC
```

Here's ASAN Report.

```
=================================================================
==8448==ERROR: AddressSanitizer: global-buffer-overflow on address 0x0000042647ec
at pc 0x000001e91b6d bp 0x7fff077c79c0 sp 0x7fff077c79b8
READ of size 4 at 0x0000042647ec thread T0
    #0 0x1e91b6c in epsc_print_page ghostpdl/./devices/gdevepsc.c:186:10
    #1 0x13f07d9 in gx_default_print_page_copies ghostpdl/./base/gdevprn.c:1231:12
    #2 0x13ef028 in gdev_prn_output_page_aux ghostpdl/./base/gdevprn.c:1133:27
    #3 0x22b6f20 in gs_output_page ghostpdl/./base/gsdevice.c:212:17
    #4 0x3054b9f in zoutputpage ghostpdl/./psi/zdevice.c:416:12
    #5 0x2e8bdb6 in interp ghostpdl/./psi/interp.c:1300:28
    #6 0x2e8bdb6 in gs_call_interp ghostpdl/./psi/interp.c:520
    #7 0x2e8bdb6 in gs_interpret ghostpdl/./psi/interp.c:477
    #8 0x2e3f451 in gs_main_interpret ghostpdl/./psi/imain.c:253:12
    #9 0x2e3f451 in gs_main_run_string_end ghostpdl/./psi/imain.c:791
    #10 0x2e3f451 in gs_main_run_string_with_length ghostpdl/./psi/imain.c:735
    #11 0x2e548f0 in run_string ghostpdl/./psi/imainarg.c:1117:12
    #12 0x2e548f0 in runarg ghostpdl/./psi/imainarg.c:1086
    #13 0x2e5302a in argproc ghostpdl/./psi/imainarg.c:1008:16
    #14 0x2e479f7 in gs_main_init_with_args01 ghostpdl/./psi/imainarg.c:241:24
    #15 0x2e539d0 in gs_main_init_with_args ghostpdl/./psi/imainarg.c:288:16
    #16 0x57b86f in main ghostpdl/./psi/gs.c:95:16
    #17 0x7ffa8af0eb96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #18 0x482e79 in _start (gs+0x482e79)

0x0000042647ec is located 20 bytes to the left of global variable '<string
literal>' defined in './devices/gdevepsc.c:178:18' (0x4264800) of size 20
  '<string literal>' is ascii string 'epsc_print_page(in)'
0x0000042647ec is located 16 bytes to the right of global variable
'graphics_modes_24' defined in './devices/gdevepsc.c:169:16' (0x42647c0) of size 28
SUMMARY: AddressSanitizer: global-buffer-overflow
ghostpdl/./devices/gdevepsc.c:186:10 in epsc_print_page
Shadow bytes around the buggy address:
  0x0000808448a0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000808448b0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000808448c0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000808448d0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000808448e0: f9 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9
=>0x0000808448f0: 00 00 04 f9 f9 f9 f9 f9 00 00 00 04 f9[f9]f9 f9
  0x000080844900: 00 00 04 f9 f9 f9 f9 f9 00 00 05 f9 f9 f9 f9 f9
  0x000080844910: 00 07 f9 f9 f9 f9 f9 f9 00 00 07 f9 f9 f9 f9 f9
  0x000080844920: 04 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9
  0x000080844930: 05 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9
  0x000080844940: 04 f9 f9 f9 f9 f9 f9 f9 00 00 05 f9 f9 f9 f9 f9
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
==8448==ABORTING
```

Julian Smith 2019-10-30 09:50:54 UTC — Comment 1

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=89f58f1aa95b3482cadf6977da49457194ee5358