Bug 701844 - heap-buffer-overflow at devices/gdevlp8k.c:330 in lp8000_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: 2019-11-05 17:09 UTC by Suhwan
Modified: 2019-11-06 16:54 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (4.96 MB, application/pdf) 2019-11-05 17:09 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 2019-11-05 17:09:00 UTC Description

Created attachment 18449 [details]
poc

Hello

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

OS: Ubuntu 18.04 64bit
Version: commit 1159afbcad927e1a32008b0ab87e257fc21da8e2

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 -dFIXEDMEDIA -sPAPERSIZE=legal -sOutputFile=tmp -
sDEVICE=lp8000 $PoC
```

Here's ASAN report.

```
==10047==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61300000116f at
pc 0x5611f64b6f91 bp 0x7fff9b6c3120 sp 0x7fff9b6c3110
WRITE of size 1 at 0x61300000116f thread T0
    #0 0x5611f64b6f90 in lp8000_print_page devices/gdevlp8k.c:330
    #1 0x5611f5f4ca02 in gx_default_print_page_copies base/gdevprn.c:1231
    #2 0x5611f5f4c3d1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #3 0x5611f5f4c6cb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #4 0x5611f662a83e in gs_output_page base/gsdevice.c:212
    #5 0x5611f6c89e6b in zoutputpage psi/zdevice.c:416
    #6 0x5611f6ba6bc6 in do_call_operator psi/interp.c:86
    #7 0x5611f6bb0345 in interp psi/interp.c:1300
    #8 0x5611f6ba8713 in gs_call_interp psi/interp.c:520
    #9 0x5611f6ba7db8 in gs_interpret psi/interp.c:477
    #10 0x5611f6b7c30f in gs_main_interpret psi/imain.c:253
    #11 0x5611f6b7f7c4 in gs_main_run_string_end psi/imain.c:791
    #12 0x5611f6b7f189 in gs_main_run_string_with_length psi/imain.c:735
    #13 0x5611f6b7f0fb in gs_main_run_string psi/imain.c:716
    #14 0x5611f6b8bdbf in run_string psi/imainarg.c:1117
    #15 0x5611f6b8bb62 in runarg psi/imainarg.c:1086
    #16 0x5611f6b8b3e1 in argproc psi/imainarg.c:1008
    #17 0x5611f6b85bad in gs_main_init_with_args01 psi/imainarg.c:241
    #18 0x5611f6b86011 in gs_main_init_with_args psi/imainarg.c:288
    #19 0x5611f6b91541 in psapi_init_with_args psi/psapi.c:272
    #20 0x5611f6d60b71 in gsapi_init_with_args psi/iapi.c:148
    #21 0x5611f5930ef8 in main psi/gs.c:95
    #22 0x7f7618c50b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #23 0x5611f5930c99 in _start (gs+0x36cc99)

0x61300000116f is located 0 bytes to the right of 367-byte region
[0x613000001000,0x61300000116f)
allocated by thread T0 here:
    #0 0x7f761a53ab50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x5611f6690297 in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x5611f66907a4 in gs_heap_alloc_byte_array base/gsmalloc.c:252
    #3 0x5611f64b6279 in lp8000_print_page devices/gdevlp8k.c:188
    #4 0x5611f5f4ca02 in gx_default_print_page_copies base/gdevprn.c:1231
    #5 0x5611f5f4c3d1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #6 0x5611f5f4c6cb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #7 0x5611f662a83e in gs_output_page base/gsdevice.c:212
    #8 0x5611f6c89e6b in zoutputpage psi/zdevice.c:416
    #9 0x5611f6ba6bc6 in do_call_operator psi/interp.c:86
    #10 0x5611f6bb0345 in interp psi/interp.c:1300
    #11 0x5611f6ba8713 in gs_call_interp psi/interp.c:520
    #12 0x5611f6ba7db8 in gs_interpret psi/interp.c:477
    #13 0x5611f6b7c30f in gs_main_interpret psi/imain.c:253
    #14 0x5611f6b7f7c4 in gs_main_run_string_end psi/imain.c:791
    #15 0x5611f6b7f189 in gs_main_run_string_with_length psi/imain.c:735
    #16 0x5611f6b7f0fb in gs_main_run_string psi/imain.c:716
    #17 0x5611f6b8bdbf in run_string psi/imainarg.c:1117
    #18 0x5611f6b8bb62 in runarg psi/imainarg.c:1086
    #19 0x5611f6b8b3e1 in argproc psi/imainarg.c:1008
    #20 0x5611f6b85bad in gs_main_init_with_args01 psi/imainarg.c:241
    #21 0x5611f6b86011 in gs_main_init_with_args psi/imainarg.c:288
    #22 0x5611f6b91541 in psapi_init_with_args psi/psapi.c:272
    #23 0x5611f6d60b71 in gsapi_init_with_args psi/iapi.c:148
    #24 0x5611f5930ef8 in main psi/gs.c:95
    #25 0x7f7618c50b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow devices/gdevlp8k.c:330 in
lp8000_print_page
Shadow bytes around the buggy address:
  0x0c267fff81d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c267fff81e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c267fff81f0: 00 00 00 00 00 00 07 fa fa fa fa fa fa fa fa fa
  0x0c267fff8200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c267fff8210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c267fff8220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00[07]fa fa
  0x0c267fff8230: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8250: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c267fff8260: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c267fff8270: 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
```

Julian Smith 2019-11-06 16:54:37 UTC Comment 1

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=4f6bc662909ab79e8fbe9822afb36e8a0eafc2b7