Bug 701829 - heap-buffer-overflow at devices/gdevcdj.c:1972 in ep_print_image

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 15:25 UTC by Suhwan
Modified: 2019-11-04 16:50 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (25.73 KB, application/pdf) 2019-11-02 15:25 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 15:25:48 UTC Description

Created attachment 18420 [details]
poc

Hello

I found a heap-buffer-overflow 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 -r12 -sOutputFile=tmp -sDEVICE=escp $PoC
```

Here's ASAN report.

```
==27643==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61d000011730 at
pc 0x7ff2a8c1ff54 bp 0x7ffc17215c80 sp 0x7ffc17215428
READ of size 4 at 0x61d000011730 thread T0
    #0 0x7ff2a8c1ff53  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xaff53)
    #1 0x563e84bdb397 in ep_print_image devices/gdevcdj.c:1972
    #2 0x563e84be1f0f in hp_colour_print_page devices/gdevcdj.c:2742
    #3 0x563e84bd8c56 in escp_print_page devices/gdevcdj.c:1344
    #4 0x563e84731302 in gx_default_print_page_copies base/gdevprn.c:1231
    #5 0x563e84730cd1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #6 0x563e84730fcb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #7 0x563e84e0ea25 in gs_output_page base/gsdevice.c:212
    #8 0x563e8546dfce in zoutputpage psi/zdevice.c:416
    #9 0x563e8538ad3a in do_call_operator psi/interp.c:86
    #10 0x563e853944b9 in interp psi/interp.c:1300
    #11 0x563e8538c887 in gs_call_interp psi/interp.c:520
    #12 0x563e8538bf2c in gs_interpret psi/interp.c:477
    #13 0x563e85360483 in gs_main_interpret psi/imain.c:253
    #14 0x563e85363938 in gs_main_run_string_end psi/imain.c:791
    #15 0x563e853632fd in gs_main_run_string_with_length psi/imain.c:735
    #16 0x563e8536326f in gs_main_run_string psi/imain.c:716
    #17 0x563e8536ff33 in run_string psi/imainarg.c:1117
    #18 0x563e8536fcd6 in runarg psi/imainarg.c:1086
    #19 0x563e8536f555 in argproc psi/imainarg.c:1008
    #20 0x563e85369d21 in gs_main_init_with_args01 psi/imainarg.c:241
    #21 0x563e8536a185 in gs_main_init_with_args psi/imainarg.c:288
    #22 0x563e853756b5 in psapi_init_with_args psi/psapi.c:272
    #23 0x563e85544cd4 in gsapi_init_with_args psi/iapi.c:148
    #24 0x563e841157f8 in main psi/gs.c:95
    #25 0x7ff2a7364b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #26 0x563e84115599 in _start (gs+0x36c599)

0x61d000011730 is located 0 bytes to the right of 2224-byte region
[0x61d000010e80,0x61d000011730)
allocated by thread T0 here:
    #0 0x7ff2a8c4eb50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x563e84e7447e in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x563e84e7498b in gs_heap_alloc_byte_array base/gsmalloc.c:252
    #3 0x563e84bdc0e2 in hp_colour_print_page devices/gdevcdj.c:2098
    #4 0x563e84bd8c56 in escp_print_page devices/gdevcdj.c:1344
    #5 0x563e84731302 in gx_default_print_page_copies base/gdevprn.c:1231
    #6 0x563e84730cd1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #7 0x563e84730fcb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #8 0x563e84e0ea25 in gs_output_page base/gsdevice.c:212
    #9 0x563e8546dfce in zoutputpage psi/zdevice.c:416
    #10 0x563e8538ad3a in do_call_operator psi/interp.c:86
    #11 0x563e853944b9 in interp psi/interp.c:1300
    #12 0x563e8538c887 in gs_call_interp psi/interp.c:520
    #13 0x563e8538bf2c in gs_interpret psi/interp.c:477
    #14 0x563e85360483 in gs_main_interpret psi/imain.c:253
    #15 0x563e85363938 in gs_main_run_string_end psi/imain.c:791
    #16 0x563e853632fd in gs_main_run_string_with_length psi/imain.c:735
    #17 0x563e8536326f in gs_main_run_string psi/imain.c:716
    #18 0x563e8536ff33 in run_string psi/imainarg.c:1117
    #19 0x563e8536fcd6 in runarg psi/imainarg.c:1086
    #20 0x563e8536f555 in argproc psi/imainarg.c:1008
    #21 0x563e85369d21 in gs_main_init_with_args01 psi/imainarg.c:241
    #22 0x563e8536a185 in gs_main_init_with_args psi/imainarg.c:288
    #23 0x563e853756b5 in psapi_init_with_args psi/psapi.c:272
    #24 0x563e85544cd4 in gsapi_init_with_args psi/iapi.c:148
    #25 0x563e841157f8 in main psi/gs.c:95
    #26 0x7ff2a7364b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xaff53)
Shadow bytes around the buggy address:
  0x0c3a7fffa290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a7fffa2a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a7fffa2b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a7fffa2c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3a7fffa2d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
=>0x0c3a7fffa2e0: 00 00 00 00 00 00[fa]fa fa fa fa fa fa fa fa
  0x0c3a7fffa2f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fffa300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fffa310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fffa320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a7fffa330: 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 2019-11-04 16:50:37 UTC Comment 1

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=af004276fd8f6c305727183c159b83021020f7d6