Bug 701819 - heap-buffer-overflow at devices/gdevpcx.c:445 in pcx_write_rle

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 18:13 UTC by Suhwan
Modified: 2019-11-04 12:46 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (25.35 KB, application/pdf) 2019-10-31 18:13 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 18:13:56 UTC Description

Created attachment 18403 [details]
poc

Hello

I found a heap-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 -r965 -sOutputFile=tmp -sDEVICE=pcx16 $PoC
```

Here's ASAN report.

```
==27944==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x622000001570 at
pc 0x556a0e09dc3f bp 0x7ffde5496af0 sp 0x7ffde5496ae0
READ of size 1 at 0x622000001570 thread T0
    #0 0x556a0e09dc3e in pcx_write_rle devices/gdevpcx.c:445
    #1 0x556a0e09d969 in pcx_write_page devices/gdevpcx.c:398
    #2 0x556a0e09c339 in pcx16_print_page devices/gdevpcx.c:257
    #3 0x556a0dc61ac5 in gx_default_print_page_copies base/gdevprn.c:1231
    #4 0x556a0dc61494 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #5 0x556a0dc6178e in gdev_prn_bg_output_page base/gdevprn.c:1181
    #6 0x556a0e33edcd in gs_output_page base/gsdevice.c:212
    #7 0x556a0e99e376 in zoutputpage psi/zdevice.c:416
    #8 0x556a0e8bb0e2 in do_call_operator psi/interp.c:86
    #9 0x556a0e8c4861 in interp psi/interp.c:1300
    #10 0x556a0e8bcc2f in gs_call_interp psi/interp.c:520
    #11 0x556a0e8bc2d4 in gs_interpret psi/interp.c:477
    #12 0x556a0e89082b in gs_main_interpret psi/imain.c:253
    #13 0x556a0e893ce0 in gs_main_run_string_end psi/imain.c:791
    #14 0x556a0e8936a5 in gs_main_run_string_with_length psi/imain.c:735
    #15 0x556a0e893617 in gs_main_run_string psi/imain.c:716
    #16 0x556a0e8a02db in run_string psi/imainarg.c:1117
    #17 0x556a0e8a007e in runarg psi/imainarg.c:1086
    #18 0x556a0e89f8fd in argproc psi/imainarg.c:1008
    #19 0x556a0e89a0c9 in gs_main_init_with_args01 psi/imainarg.c:241
    #20 0x556a0e89a52d in gs_main_init_with_args psi/imainarg.c:288
    #21 0x556a0e8a5a5d in psapi_init_with_args psi/psapi.c:272
    #22 0x556a0ea7507c in gsapi_init_with_args psi/iapi.c:148
    #23 0x556a0d6461d8 in main psi/gs.c:95
    #24 0x7f26d2b01b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #25 0x556a0d645f79 in _start (gs+0x36bf79)

0x622000001570 is located 0 bytes to the right of 5232-byte region
[0x622000000100,0x622000001570)
allocated by thread T0 here:
    #0 0x7f26d43ebb50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x556a0e3a4826 in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x556a0e31417b in alloc_acquire_clump base/gsalloc.c:2485
    #3 0x556a0e311422 in alloc_obj base/gsalloc.c:1948
    #4 0x556a0e30c125 in i_alloc_bytes base/gsalloc.c:1176
    #5 0x556a0e09d0b4 in pcx_write_page devices/gdevpcx.c:331
    #6 0x556a0e09c339 in pcx16_print_page devices/gdevpcx.c:257
    #7 0x556a0dc61ac5 in gx_default_print_page_copies base/gdevprn.c:1231
    #8 0x556a0dc61494 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #9 0x556a0dc6178e in gdev_prn_bg_output_page base/gdevprn.c:1181
    #10 0x556a0e33edcd in gs_output_page base/gsdevice.c:212
    #11 0x556a0e99e376 in zoutputpage psi/zdevice.c:416
    #12 0x556a0e8bb0e2 in do_call_operator psi/interp.c:86
    #13 0x556a0e8c4861 in interp psi/interp.c:1300
    #14 0x556a0e8bcc2f in gs_call_interp psi/interp.c:520
    #15 0x556a0e8bc2d4 in gs_interpret psi/interp.c:477
    #16 0x556a0e89082b in gs_main_interpret psi/imain.c:253
    #17 0x556a0e893ce0 in gs_main_run_string_end psi/imain.c:791
    #18 0x556a0e8936a5 in gs_main_run_string_with_length psi/imain.c:735
    #19 0x556a0e893617 in gs_main_run_string psi/imain.c:716
    #20 0x556a0e8a02db in run_string psi/imainarg.c:1117
    #21 0x556a0e8a007e in runarg psi/imainarg.c:1086
    #22 0x556a0e89f8fd in argproc psi/imainarg.c:1008
    #23 0x556a0e89a0c9 in gs_main_init_with_args01 psi/imainarg.c:241
    #24 0x556a0e89a52d in gs_main_init_with_args psi/imainarg.c:288
    #25 0x556a0e8a5a5d in psapi_init_with_args psi/psapi.c:272
    #26 0x556a0ea7507c in gsapi_init_with_args psi/iapi.c:148
    #27 0x556a0d6461d8 in main psi/gs.c:95
    #28 0x7f26d2b01b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow devices/gdevpcx.c:445 in
pcx_write_rle
Shadow bytes around the buggy address:
  0x0c447fff8250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c447fff8290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c447fff82a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa
  0x0c447fff82b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82f0: 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 12:46:15 UTC Comment 1

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=2793769ff107d8d22dadd30c6e68cd781b569550