Bug 701816 - heap-buffer-overflow at base/gxicolor.c:957 in image_render_color_thresh

Status: RESOLVED FIXED
Alias: None
Product: Ghostscript
Component: Images (show other bugs)
Version: master
Hardware: PC Linux
Importance: P4 normal
Assignee: Robin Watts
URL:
Keywords:
Depends on:
Blocks:

Reported: 2019-10-31 18:03 UTC by Suhwan
Modified: 2019-11-05 19:26 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (13.27 KB, image/x-eps) 2019-10-31 18:03 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 18:03:38 UTC Description

Created attachment 18400 [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 -dFitPage -sOutputFile=tmp -sDEVICE=plank $PoC
Here's ASAN report.

==17311==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fa1955a6730 at
pc 0x56189b3f497d bp 0x7ffcf93e73b0 sp 0x7ffcf93e73a0
WRITE of size 1 at 0x7fa1955a6730 thread T0
    #0 0x56189b3f497c in image_render_color_thresh base/gxicolor.c:957
    #1 0x56189c39ffed in gx_image1_plane_data base/gxidata.c:237
    #2 0x56189c3a86a8 in gx_image_plane_data_rows base/gximage.c:183
    #3 0x56189c0688fb in gs_image_next_planes base/gsimage.c:621
    #4 0x56189c68bc31 in image_proc_continue psi/zimage.c:442
    #5 0x56189c5930e2 in do_call_operator psi/interp.c:86
    #6 0x56189c59c861 in interp psi/interp.c:1300
    #7 0x56189c594c2f in gs_call_interp psi/interp.c:520
    #8 0x56189c5942d4 in gs_interpret psi/interp.c:477
    #9 0x56189c56882b in gs_main_interpret psi/imain.c:253
    #10 0x56189c56bce0 in gs_main_run_string_end psi/imain.c:791
    #11 0x56189c56b6a5 in gs_main_run_string_with_length psi/imain.c:735
    #12 0x56189c56b617 in gs_main_run_string psi/imain.c:716
    #13 0x56189c5782db in run_string psi/imainarg.c:1117
    #14 0x56189c57807e in runarg psi/imainarg.c:1086
    #15 0x56189c5778fd in argproc psi/imainarg.c:1008
    #16 0x56189c5720c9 in gs_main_init_with_args01 psi/imainarg.c:241
    #17 0x56189c57252d in gs_main_init_with_args psi/imainarg.c:288
    #18 0x56189c57da5d in psapi_init_with_args psi/psapi.c:272
    #19 0x56189c74d07c in gsapi_init_with_args psi/iapi.c:148
    #20 0x56189b31e1d8 in main psi/gs.c:95
    #21 0x7fa19e27ab96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #22 0x56189b31df79 in _start (gs+0x36bf79)

0x7fa1955a6730 is located 208 bytes to the left of 671864-byte region
[0x7fa1955a6800,0x7fa19564a878)
allocated by thread T0 here:
    #0 0x7fa19fb64b50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x56189c07c826 in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x56189bfec17b in alloc_acquire_clump base/gsalloc.c:2485
    #3 0x56189bfe9422 in alloc_obj base/gsalloc.c:1948
    #4 0x56189bfe4125 in i_alloc_bytes base/gsalloc.c:1176
    #5 0x56189c399038 in gxht_thresh_image_init base/gxht_thresh.c:635
    #6 0x56189b3ee3e2 in gs_image_class_4_color base/gxicolor.c:299
    #7 0x56189c3c4cd7 in gx_image_enum_begin base/gxipixel.c:1019
    #8 0x56189c3ad15a in gx_begin_image1 base/gximage1.c:94
    #9 0x56189c44c0d1 in gx_default_begin_typed_image base/gdevddrw.c:1052
    #10 0x56189c44bdb2 in gx_default_begin_image base/gdevddrw.c:1021
    #11 0x56189c44c04b in gx_default_begin_typed_image base/gdevddrw.c:1044
    #12 0x56189b96a1d2 in epo_begin_typed_image base/gdevepo.c:538
    #13 0x56189c0651ab in gs_image_begin_typed base/gsimage.c:258
    #14 0x56189c6898ea in zimage_setup psi/zimage.c:180
    #15 0x56189c689ff9 in zimage1 psi/zimage.c:243
    #16 0x56189c5930e2 in do_call_operator psi/interp.c:86
    #17 0x56189c59fd13 in interp psi/interp.c:1674
    #18 0x56189c594c2f in gs_call_interp psi/interp.c:520
    #19 0x56189c5942d4 in gs_interpret psi/interp.c:477
    #20 0x56189c56882b in gs_main_interpret psi/imain.c:253
    #21 0x56189c56bce0 in gs_main_run_string_end psi/imain.c:791
    #22 0x56189c56b6a5 in gs_main_run_string_with_length psi/imain.c:735
    #23 0x56189c56b617 in gs_main_run_string psi/imain.c:716
    #24 0x56189c5782db in run_string psi/imainarg.c:1117
    #25 0x56189c57807e in runarg psi/imainarg.c:1086
    #26 0x56189c5778fd in argproc psi/imainarg.c:1008
    #27 0x56189c5720c9 in gs_main_init_with_args01 psi/imainarg.c:241
    #28 0x56189c57252d in gs_main_init_with_args psi/imainarg.c:288
    #29 0x56189c57da5d in psapi_init_with_args psi/psapi.c:272

SUMMARY: AddressSanitizer: heap-buffer-overflow base/gxicolor.c:957 in
image_render_color_thresh
Shadow bytes around the buggy address:
  0x0ff4b2aacc90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4b2aacca0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4b2aaccb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4b2aaccc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4b2aaccd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0ff4b2aacce0: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa
  0x0ff4b2aaccf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff4b2aacd00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0ff4b2aacd10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff4b2aacd20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff4b2aacd30: 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
```

Robin Watts **2019-11-05 19:26:12 UTC** **Comment 1**

Fixed in:

```
commit 027c546e0dd11e0526f1780a7f3c2c66acffe209 (golden/master)
Author: Robin Watts <Robin.Watts@artifex.com>
Date:   Tue Nov 5 18:18:50 2019 +0000

    Bug 701843: Fix misindexing in gxicolor.c

    We were incorrectly decrementing position per-component, rather
    than per-pixel (in 2 places).

    Also, take care of some whitespace oddities.

Apologies for the wrong bug number in the commit message.
```