Bug 701807 - heap-buffer-overflow at devices/gdevtfnx.c:170 in tiff12_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: 2019-10-29 07:51 UTC by Suhwan
Modified: 2019-10-31 12:03 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (7.84 KB, application/pdf) 2019-10-29 07:51 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 2019-10-29 07:51:49 UTC Description

Created attachment 18389 [details]
poc

Hello

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

OS: Ubuntu 18.04 64bit
Version: commit 6e6c69487094b877bc56fcc07b9840f6e5b95925

Steps to reproduce:
1. Download the .POC files.
2. Compile the source code with "make sanitize" using gcc.
3. Run following cmd.

```
gs -r650 -sOutputFile=tmp -sDEVICE=tiff12nc $PoC
```

Here's ASAN report.

```
==31742==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x629000072328 at
pc 0x560ef9c76b37 bp 0x7ffda8ac4b80 sp 0x7ffda8ac4b70
READ of size 1 at 0x629000072328 thread T0
    #0 0x560ef9c76b36 in tiff12_print_page devices/gdevtfnx.c:170
    #1 0x560ef982a3f5 in gx_default_print_page_copies base/gdevprn.c:1231
    #2 0x560ef9829dc4 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #3 0x560ef982a08d in gdev_prn_output_page_seekable base/gdevprn.c:1175
    #4 0x560ef9f0737b in gs_output_page base/gsdevice.c:212
    #5 0x560efa566924 in zoutputpage psi/zdevice.c:416
    #6 0x560efa483690 in do_call_operator psi/interp.c:86
    #7 0x560efa48ce0f in interp psi/interp.c:1300
    #8 0x560efa4851dd in gs_call_interp psi/interp.c:520
    #9 0x560efa484882 in gs_interpret psi/interp.c:477
    #10 0x560efa458dd9 in gs_main_interpret psi/imain.c:253
    #11 0x560efa45c28e in gs_main_run_string_end psi/imain.c:791
    #12 0x560efa45bc53 in gs_main_run_string_with_length psi/imain.c:735
    #13 0x560efa45bbc5 in gs_main_run_string psi/imain.c:716
    #14 0x560efa468889 in run_string psi/imainarg.c:1117
    #15 0x560efa46862c in runarg psi/imainarg.c:1086
    #16 0x560efa467eab in argproc psi/imainarg.c:1008
    #17 0x560efa462677 in gs_main_init_with_args01 psi/imainarg.c:241
    #18 0x560efa462adb in gs_main_init_with_args psi/imainarg.c:288
    #19 0x560efa46e00b in psapi_init_with_args psi/psapi.c:272
    #20 0x560efa63d62a in gsapi_init_with_args psi/iapi.c:148
    #21 0x560ef920eb08 in main psi/gs.c:95
    #22 0x7efe4aac3b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #23 0x560ef920e8a9 in _start (gs+0x36b8a9)

0x629000072328 is located 0 bytes to the right of 16680-byte region
[0x62900006e200,0x629000072328)
allocated by thread T0 here:
    #0 0x7efe4c3adb50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x560ef9f6cdd4 in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x560ef9edc729 in alloc_acquire_clump base/gsalloc.c:2485
    #3 0x560ef9ed99d0 in alloc_obj base/gsalloc.c:1948
    #4 0x560ef9ed46d3 in i_alloc_bytes base/gsalloc.c:1176
    #5 0x560ef9c768e1 in tiff12_print_page devices/gdevtfnx.c:149
    #6 0x560ef982a3f5 in gx_default_print_page_copies base/gdevprn.c:1231
    #7 0x560ef9829dc4 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #8 0x560ef982a08d in gdev_prn_output_page_seekable base/gdevprn.c:1175
    #9 0x560ef9f0737b in gs_output_page base/gsdevice.c:212
    #10 0x560efa566924 in zoutputpage psi/zdevice.c:416
    #11 0x560efa483690 in do_call_operator psi/interp.c:86
    #12 0x560efa48ce0f in interp psi/interp.c:1300
    #13 0x560efa4851dd in gs_call_interp psi/interp.c:520
    #14 0x560efa484882 in gs_interpret psi/interp.c:477
    #15 0x560efa458dd9 in gs_main_interpret psi/imain.c:253
    #16 0x560efa45c28e in gs_main_run_string_end psi/imain.c:791
    #17 0x560efa45bc53 in gs_main_run_string_with_length psi/imain.c:735
    #18 0x560efa45bbc5 in gs_main_run_string psi/imain.c:716
    #19 0x560efa468889 in run_string psi/imainarg.c:1117
    #20 0x560efa46862c in runarg psi/imainarg.c:1086
    #21 0x560efa467eab in argproc psi/imainarg.c:1008
    #22 0x560efa462677 in gs_main_init_with_args01 psi/imainarg.c:241
    #23 0x560efa462adb in gs_main_init_with_args psi/imainarg.c:288
    #24 0x560efa46e00b in psapi_init_with_args psi/psapi.c:272
    #25 0x560efa63d62a in gsapi_init_with_args psi/iapi.c:148
    #26 0x560ef920eb08 in main psi/gs.c:95
    #27 0x7efe4aac3b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow devices/gdevtfnx.c:170 in
tiff12_print_page
Shadow bytes around the buggy address:
  0x0c5280006410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5280006420: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5280006430: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5280006440: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5280006450: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c5280006460: 00 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa
  0x0c5280006470: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5280006480: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c5280006490: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c52800064a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c52800064b0: 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 **2019-10-31 12:03:01 UTC** **Comment 1**

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=714e8995cd582d418276915cbbec3c70711fb19e