Bug 701827 - heap-buffer-overflow at devices/gdevlxm.c:304 in lxm5700m_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: 2019-11-02 15:15 UTC by Suhwan
Modified: 2021-09-11 12:54 UTC (History)
CC List: 1 user (show)
See Also:
Customer:
Word Size: ---

Attachments	
poc (133.95 KB, image/x-eps) 2019-11-02 15:15 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 15:15:01 UTC **Description**

Created attachment 18418 [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 -r425 -dFitPage -sOutputFile=tmp -sDEVICE=lxm5700m $PoC
Here's ASAN report.

==27089==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x63200005f770 at
pc 0x560794413259 bp 0x7fffd7e2a080 sp 0x7fffd7e2a070
WRITE of size 1 at 0x63200005f770 thread T0
    #0 0x560794413258 in lxm5700m_print_page devices/gdevlxm.c:304
    #1 0x560793e95302 in gx_default_print_page_copies base/gdevprn.c:1231
    #2 0x560793e94cd1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #3 0x560793e94fcb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #4 0x560794572a25 in gs_output_page base/gsdevice.c:212
    #5 0x560794bd1fce in zoutputpage psi/zdevice.c:416
    #6 0x560794aeed3a in do_call_operator psi/interp.c:86
    #7 0x560794af84b9 in interp psi/interp.c:1300
    #8 0x560794af0887 in gs_call_interp psi/interp.c:520
    #9 0x560794aeff2c in gs_interpret psi/interp.c:477
    #10 0x560794ac4483 in gs_main_interpret psi/imain.c:253
    #11 0x560794ac7938 in gs_main_run_string_end psi/imain.c:791
    #12 0x560794ac72fd in gs_main_run_string_with_length psi/imain.c:735
    #13 0x560794ac726f in gs_main_run_string psi/imain.c:716
    #14 0x560794ad3f33 in run_string psi/imainarg.c:1117
    #15 0x560794ad3cd6 in runarg psi/imainarg.c:1086
    #16 0x560794ad3555 in argproc psi/imainarg.c:1008
    #17 0x560794acdd21 in gs_main_init_with_args01 psi/imainarg.c:241
    #18 0x560794ace185 in gs_main_init_with_args psi/imainarg.c:288
    #19 0x560794ad96b5 in psapi_init_with_args psi/psapi.c:272
    #20 0x560794ca8cd4 in gsapi_init_with_args psi/iapi.c:148
    #21 0x5607938797f8 in main psi/gs.c:95
    #22 0x7fbbb17a6b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #23 0x560793879599 in _start (gs+0x36c599)

0x63200005f770 is located 0 bytes to the right of 94064-byte region
[0x632000048800,0x63200005f770)
freed by thread T0 here:
    #0 0x7fbbb30907b8 in __interceptor_free (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xde7b8)
    #1 0x5607945d93c4 in gs_heap_free_object base/gsmalloc.c:358
    #2 0x560794413669 in lxm5700m_print_page devices/gdevlxm.c:308
    #3 0x560793e95302 in gx_default_print_page_copies base/gdevprn.c:1231
    #4 0x560793e94cd1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #5 0x560793e94fcb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #6 0x560794572a25 in gs_output_page base/gsdevice.c:212
    #7 0x560794bd1fce in zoutputpage psi/zdevice.c:416
    #8 0x560794aeed3a in do_call_operator psi/interp.c:86
    #9 0x560794af84b9 in interp psi/interp.c:1300
    #10 0x560794af0887 in gs_call_interp psi/interp.c:520
    #11 0x560794aeff2c in gs_interpret psi/interp.c:477
    #12 0x560794ac4483 in gs_main_interpret psi/imain.c:253
    #13 0x560794ac7938 in gs_main_run_string_end psi/imain.c:791
    #14 0x560794ac72fd in gs_main_run_string_with_length psi/imain.c:735
    #15 0x560794ac726f in gs_main_run_string psi/imain.c:716
    #16 0x560794ad3f33 in run_string psi/imainarg.c:1117
    #17 0x560794ad3cd6 in runarg psi/imainarg.c:1086
    #18 0x560794ad3555 in argproc psi/imainarg.c:1008
    #19 0x560794acdd21 in gs_main_init_with_args01 psi/imainarg.c:241
    #20 0x560794ace185 in gs_main_init_with_args psi/imainarg.c:288
    #21 0x560794ad96b5 in psapi_init_with_args psi/psapi.c:272
    #22 0x560794ca8cd4 in gsapi_init_with_args psi/iapi.c:148
    #23 0x5607938797f8 in main psi/gs.c:95
    #24 0x7fbbb17a6b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

previously allocated by thread T0 here:
    #0 0x7fbbb3090b50 in __interceptor_malloc (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xdeb50)
    #1 0x5607945d847e in gs_heap_alloc_bytes base/gsmalloc.c:193
    #2 0x5607945d898b in gs_heap_alloc_byte_array base/gsmalloc.c:252
    #3 0x560794412252f in lxm5700m_print_page devices/gdevlxm.c:155
    #4 0x560793e95302 in gx_default_print_page_copies base/gdevprn.c:1231
    #5 0x560793e94cd1 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #6 0x560793e94fcb in gdev_prn_bg_output_page base/gdevprn.c:1181
    #7 0x560794572a25 in gs_output_page base/gsdevice.c:212
    #8 0x560794bd1fce in zoutputpage psi/zdevice.c:416
    #9 0x560794aeed3a in do_call_operator psi/interp.c:86
    #10 0x560794af84b9 in interp psi/interp.c:1300
    #11 0x560794af0887 in gs_call_interp psi/interp.c:520
```

```
    #12 0x560794aeff2c in gs_interpret psi/interp.c:477
    #13 0x560794ac4483 in gs_main_interpret psi/imain.c:253
    #14 0x560794ac7938 in gs_main_run_string_end psi/imain.c:791
    #15 0x560794ac72fd in gs_main_run_string_with_length psi/imain.c:735
    #16 0x560794ac726f in gs_main_run_string psi/imain.c:716
    #17 0x560794ad3f33 in run_string psi/imainarg.c:1117
    #18 0x560794ad3cd6 in runarg psi/imainarg.c:1086
    #19 0x560794ad3555 in argproc psi/imainarg.c:1008
    #20 0x560794acdd21 in gs_main_init_with_args01 psi/imainarg.c:241
    #21 0x560794ace185 in gs_main_init_with_args psi/imainarg.c:288
    #22 0x560794ad96b5 in psapi_init_with_args psi/psapi.c:272
    #23 0x560794ca8cd4 in gsapi_init_with_args psi/iapi.c:148
    #24 0x5607938797f8 in main psi/gs.c:95
    #25 0x7fbbb17a6b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow devices/gdevlxm.c:304 in
lxm5700m_print_page
Shadow bytes around the buggy address:
  0x0c6480003e90: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c6480003ea0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c6480003eb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c6480003ec0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c6480003ed0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c6480003ee0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fa]fa
  0x0c6480003ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c6480003f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c6480003f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c6480003f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c6480003f30: 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
```

Ken Sharp 2019-11-02 15:26:01 UTC Comment 1

Probably needs code to prevent the resolution being changed. Just guessing, but its probably a fixed resolution device, 600 dpi, the comments say 1200 but the device setup has 600.

In any event -r425 should throw a rangecheck error.

Julian Smith 2019-11-04 14:37:18 UTC Comment 2

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=a6f7464dddc689386668a38b92dfd03cc1b38a10