Bug 701788 - heap-buffer-overflow at devices/gdevcif.c:64 in cif_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: 2019-10-26 05:41 UTC by Suhwan
Modified: 2021-10-30 08:17 UTC (History)
CC List: 1 user (show)
See Also:
Customer:
Word Size: ---

Attachments	
poc (11.25 KB, application/pdf) 2019-10-26 05:41 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 2019-10-26 05:41:09 UTC — Description

Created attachment 18372 [details]
poc

Hello.

I found a heap-buffer-overflow bug in GhostScript.

Please confirm.

Thanks.

OS: Ubuntu 18.04 64bit

Steps to reproduce:
1. Download the .POC files.
2. Compile the source code with ASan.
3. Run following cmd.

```
gs -sOutputFile=tmp -sDEVICE=cif $PoC
```

Here's ASAN report

```
=================================================================
==9496==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x606000001d9a at
pc 0x000001883541 bp 0x7ffded5d4480 sp 0x7ffded5d4478
WRITE of size 1 at 0x606000001d9a thread T0
    #0 0x1883540 in cif_print_page ghostpdl/./devices/gdevcif.c:64:23
    #1 0x13f07d9 in gx_default_print_page_copies ghostpdl/./base/gdevprn.c:1231:12
    #2 0x13ef028 in gdev_prn_output_page_aux ghostpdl/./base/gdevprn.c:1133:27
    #3 0x22b6f20 in gs_output_page ghostpdl/./base/gsdevice.c:212:17
    #4 0x3054b9f in zoutputpage ghostpdl/./psi/zdevice.c:416:12
    #5 0x2e8bdb6 in interp ghostpdl/./psi/interp.c:1300:28
    #6 0x2e8bdb6 in gs_call_interp ghostpdl/./psi/interp.c:520
    #7 0x2e8bdb6 in gs_interpret ghostpdl/./psi/interp.c:477
    #8 0x2e3f451 in gs_main_interpret ghostpdl/./psi/imain.c:253:12
    #9 0x2e3f451 in gs_main_run_string_end ghostpdl/./psi/imain.c:791
    #10 0x2e3f451 in gs_main_run_string_with_length ghostpdl/./psi/imain.c:735
    #11 0x2e548f0 in run_string ghostpdl/./psi/imainarg.c:1117:12
    #12 0x2e548f0 in runarg ghostpdl/./psi/imainarg.c:1086
    #13 0x2e5302a in argproc ghostpdl/./psi/imainarg.c:1008:16
    #14 0x2e479f7 in gs_main_init_with_args01 ghostpdl/./psi/imainarg.c:241:24
    #15 0x2e539d0 in gs_main_init_with_args ghostpdl/./psi/imainarg.c:288:16
    #16 0x57b86f in main ghostpdl/./psi/gs.c:95:16
    #17 0x7f6808d4fb96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #18 0x482e79 in _start (gs+0x482e79)

0x606000001d9a is located 0 bytes to the right of 58-byte region
[0x606000001d60,0x606000001d9a)
allocated by thread T0 here:
    #0 0x542d30 in __interceptor_malloc (gs+0x542d30)
    #1 0x23640fd in gs_heap_alloc_bytes ghostpdl/./base/gsmalloc.c:193:34

SUMMARY: AddressSanitizer: heap-buffer-overflow ghostpdl/./devices/gdevcif.c:64:23
in cif_print_page
Shadow bytes around the buggy address:
  0x0c0c7fff8360: fa fa fa fa 00 00 00 00 00 00 07 fa fa fa fa fa
  0x0c0c7fff8370: fd fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd
  0x0c0c7fff8380: fd fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd
  0x0c0c7fff8390: fa fa fa fa 00 00 00 00 00 00 00 01 fa fa fa fa
  0x0c0c7fff83a0: fd fd fd fd fd fd fd fd fd fa fa fa 00 00 00 00
=>0x0c0c7fff83b0: 00 00 00[02]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff83c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff83d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff83e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff83f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8400: 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
==9496==ABORTING
```

Julian Smith 2019-10-29 15:17:28 UTC — Comment 1

Fixed in https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=d31e25ed5b130499e0d880e4609b1b4824699768.

include space for string terminator in call to malloc in cif_print_page().