Bug 701808 - global-buffer-overflow at devices/gdevokii.c:109 in okiibm_print_page1

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 07:54 UTC by Suhwan
Modified: 2019-10-31 15:44 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (1.84 MB, application/pdf) 2019-10-29 07:54 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 07:54:53 UTC — Description

Created attachment 18390 [details]
poc

Hello

I found a global-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 -dBATCH -dNOPAUSE -dSAFER -r599 -sOutputFile=tmp -sDEVICE=okiibm $PoC
```

Here's ASAN report.

```
==33661==ERROR: AddressSanitizer: global-buffer-overflow on address 0x562db78fe609
at pc 0x562db66108e8 bp 0x7fff84c973c0 sp 0x7fff84c973b0
READ of size 1 at 0x562db78fe609 thread T0
    #0 0x562db66108e7 in okiibm_print_page1 devices/gdevokii.c:109
    #1 0x562db66118a4 in okiibm_print_page devices/gdevokii.c:319
    #2 0x562db607a3f5 in gx_default_print_page_copies base/gdevprn.c:1231
    #3 0x562db6079dc4 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #4 0x562db607a0be in gdev_prn_bg_output_page base/gdevprn.c:1181
    #5 0x562db675737b in gs_output_page base/gsdevice.c:212
    #6 0x562db6db6924 in zoutputpage psi/zdevice.c:416
    #7 0x562db6cd3690 in do_call_operator psi/interp.c:86
    #8 0x562db6cdce0f in interp psi/interp.c:1300
    #9 0x562db6cd51dd in gs_call_interp psi/interp.c:520
    #10 0x562db6cd4882 in gs_interpret psi/interp.c:477
    #11 0x562db6ca8dd9 in gs_main_interpret psi/imain.c:253
    #12 0x562db6cac28e in gs_main_run_string_end psi/imain.c:791
    #13 0x562db6cabc53 in gs_main_run_string_with_length psi/imain.c:735
    #14 0x562db6cabbc5 in gs_main_run_string psi/imain.c:716
    #15 0x562db6cb8889 in run_string psi/imainarg.c:1117
    #16 0x562db6cb862c in runarg psi/imainarg.c:1086
    #17 0x562db6cb7eab in argproc psi/imainarg.c:1008
    #18 0x562db6cb2677 in gs_main_init_with_args01 psi/imainarg.c:241
    #19 0x562db6cb2adb in gs_main_init_with_args psi/imainarg.c:288
    #20 0x562db6cbe00b in psapi_init_with_args psi/psapi.c:272
    #21 0x562db6e8d62a in gsapi_init_with_args psi/iapi.c:148
    #22 0x562db5a5eb08 in main psi/gs.c:95
    #23 0x7f8dc12c1b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #24 0x562db5a5e8a9 in _start (gs+0x36b8a9)

0x562db78fe609 is located 4 bytes to the right of global variable
'graphics_modes_9' defined in './devices/gdevokii.c:94:27' (0x562db78fe600) of size
5
0x562db78fe609 is located 55 bytes to the left of global variable 'index' defined
in './devices/gdevokii.c:185:43' (0x562db78fe640) of size 16
SUMMARY: AddressSanitizer: global-buffer-overflow devices/gdevokii.c:109 in
okiibm_print_page1
Shadow bytes around the buggy address:
  0x0ac636f17c70: 00 00 00 f9 f9 f9 f9 f9 00 00 05 f9 f9 f9 f9 f9
  0x0ac636f17c80: 05 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0ac636f17c90: 05 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ac636f17ca0: 01 f9 f9 f9 f9 f9 f9 f9 03 f9 f9 f9 f9 f9 f9 f9
  0x0ac636f17cb0: 03 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
=>0x0ac636f17cc0: 05[f9]f9 f9 f9 f9 f9 f9 00 00 f9 f9 f9 f9 f9 f9
  0x0ac636f17cd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ac636f17ce0: 00 00 00 00 00 00 00 00 04 f9 f9 f9 f9 f9 f9 f9
  0x0ac636f17cf0: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0ac636f17d00: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0ac636f17d10: 03 f9 f9 f9 f9 f9 f9 f9 03 f9 f9 f9 f9 f9 f9 f9
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 15:44:39 UTC — Comment 1

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=f54414c8b15b2c27d1dcadd92cfe84f6d15f18dc