Bug 701785 - heap-buffer-overflow at contrib/lips4/gdevlprn.c:338 in lprn_is_black

Status: RESOLVED FIXED
Alias: None
Product: Ghostscript
Component: Valgrind/AddressSanitizer (show other bugs)
Version: master
Hardware: PC Linux
Importance: P4 normal
Assignee: Julian Smith
URL:
Keywords:
Depends on:
Blocks:

Reported: 2019-10-26 05:23 UTC by Suhwan
Modified: 2019-10-28 15:48 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (11.24 KB, application/pdf) 2019-10-26 05:23 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 05:23:38 UTC **Description**

Created attachment 18369 [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=lips2p $PoC

Here's ASAN report.

```
GPL Ghostscript GIT PRERELEASE 9.51 (2019-10-15)
Copyright (C) 2019 Artifex Software, Inc.  All rights reserved.
This software is supplied under the GNU AGPLv3 and comes with NO WARRANTY:
see the file COPYING for details.
Processing pages 1 through 1.
Page 1
=================================================================
==43099==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62f000029530 at
pc 0x000001df6f12 bp 0x7ffcd1679a30 sp 0x7ffcd1679a28
READ of size 1 at 0x62f000029530 thread T0
    #0 0x1df6f11 in lprn_is_black ghostpdl/./contrib/lips4/gdevlprn.c:338:17
    #1 0x1df6f11 in lprn_process_line ghostpdl/./contrib/lips4/gdevlprn.c:305
    #2 0x1df6f11 in lprn_print_image ghostpdl/./contrib/lips4/gdevlprn.c:260
    #3 0x1dd8051 in lips_print_page_copies
ghostpdl/./contrib/lips4/gdevl4r.c:609:12
    #4 0x13ef028 in gdev_prn_output_page_aux ghostpdl/./base/gdevprn.c:1133:27
    #5 0x22b6f20 in gs_output_page ghostpdl/./base/gsdevice.c:212:17
    #6 0x3054b9f in zoutputpage ghostpdl/./psi/zdevice.c:416:12
    #7 0x2e8bdb6 in interp ghostpdl/./psi/interp.c:1300:28
    #8 0x2e8bdb6 in gs_call_interp ghostpdl/./psi/interp.c:520
    #9 0x2e8bdb6 in gs_interpret ghostpdl/./psi/interp.c:477
    #10 0x2e3f451 in gs_main_interpret ghostpdl/./psi/imain.c:253:12
    #11 0x2e3f451 in gs_main_run_string_end ghostpdl/./psi/imain.c:791
    #12 0x2e3f451 in gs_main_run_string_with_length ghostpdl/./psi/imain.c:735
    #13 0x2e548f0 in run_string ghostpdl/./psi/imainarg.c:1117:12
    #14 0x2e548f0 in runarg ghostpdl/./psi/imainarg.c:1086
    #15 0x2e5302a in argproc ghostpdl/./psi/imainarg.c:1008:16
    #16 0x2e479f7 in gs_main_init_with_args01 ghostpdl/./psi/imainarg.c:241:24
    #17 0x2e539d0 in gs_main_init_with_args ghostpdl/./psi/imainarg.c:288:16
    #18 0x57b86f in main ghostpdl/./psi/gs.c:95:16
    #19 0x7f88b0540b96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #20 0x482e79 in _start (gs+0x482e79)

0x62f000029530 is located 0 bytes to the right of 53552-byte region
[0x62f00001c400,0x62f000029530)
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/./contrib/lips4/gdevlprn.c:338:17 in lprn_is_black
Shadow bytes around the buggy address:
  0x0c5e7fffd250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fffd260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fffd270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fffd280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5e7fffd290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c5e7fffd2a0: 00 00 00 00 00 00 00[fa]fa fa fa fa fa fa fa fa
  0x0c5e7fffd2b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fffd2c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fffd2d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fffd2e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5e7fffd2f0: 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
==43099==ABORTING
```

Julian Smith **2019-10-28 15:48:37 UTC** **Comment 1**

Fixed in: https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=450da26a76286a8342ec0864b3d113856709f8f6

~~Bug 701705~~: fixed sanitizer heap-buffer-overflow in lprn_is_black().