

Bug 701792 - heap-buffer-overflow at contrib/lips4/gdevlips.c:148 in GetNumSameData

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 06:18 UTC by Suhwan
Modified: 2019-10-30 09:49 UTC (History)
CC List: 0 users

See Also:
Customer:
Word Size: ---

Attachments	
poc (25.73 KB, application/pdf) 2019-10-26 06:18 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 06:18:17 UTC	Description
Created attachment 18376 [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=lips4v \$PoC		
Here's ASAN report.		
===== ==9464==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62a0003addf8 at pc 0x000001df0b49 bp 0x7ffebd529810 sp 0x7ffebd529808 READ of size 1 at 0x62a0003addf8 thread T0 #0 0x1df0b48 in GetNumSameData ghostpd1/./contrib/lips4/gdevlips.c:148:23 #1 0x1df0b48 in lips_packbits encode ghostpd1/./contrib/lips4/gdevlips.c:83 #2 0x1f6689f in lips4v_write_image_data ghostpd1/./contrib/lips4/gdevl4v.c:649:11 #3 0x1f4c157 in lips4v_copy_color ghostpd1/./contrib/lips4/gdevl4v.c:2110:13 #4 0x2ba6c40 in transform_pixel_region_render_portrait ghostpd1/./base/gdevdflt.c:1958:20 #5 0x2b9562e in gx_default_transform_pixel_region_process_data ghostpd1/./base/gdevdflt.c:2210:15 #6 0x2b9562e in gx_default_transform_pixel_region ghostpd1/./base/gdevdflt.c:2240 #7 0x756727 in image_render_color_icc_tpr ghostpd1/./base/gxicolor.c:1078:12 #8 0x2a0d91d in gx_image_plane_data ghostpd1/./base/gxidata.c:237:20 #9 0x2a23618 in gx_image_plane_data_rows ghostpd1/./base/gximage.c:183:12 #10 0x2a23618 in gx_image_plane_data ghostpd1/./base/gximage.c:175 #11 0x1f6795c in lips4v_image_plane_data ghostpd1/./contrib/lips4/gdevl4v.c:2424:16 #12 0x23456c1 in gs_image_next_planes ghostpd1/./base/gsimage.c:621:20 #13 0x307aa81 in image_file_continue ghostpd1/./psi/zimage.c:562:20 #14 0x2e8bdb6 in interp_ghostpd1/./psi/interp.c:1300:28 #15 0x2e8bdb6 in gs_call_interp ghostpd1/./psi/interp.c:520 #16 0x2e8bdb6 in gs_interpret_ghostpd1/./psi/interp.c:477 #17 0x2e3f451 in gs_main_interpret_ghostpd1/./psi/imain.c:253:12 #18 0x2e3f451 in gs_main_run_string_end ghostpd1/./psi/imain.c:791 #19 0x2e3f451 in gs_main_run_string_with_length ghostpd1/./psi/imain.c:735 #20 0x2e548f0 in run_string_ghostpd1/./psi/iminarg.c:1117:12 #21 0x2e548f0 in runarg_ghostpd1/./psi/iminarg.c:1086 #22 0x2e5302a in argproc_ghostpd1/./psi/iminarg.c:1008:16 #23 0x2e479f7 in gs_main_init_with_args01 ghostpd1/./psi/iminarg.c:241:24 #24 0x2e539d0 in gs_main_init_with_args ghostpd1/./psi/iminarg.c:288:16 #25 0x57b86f in main ghostpd1/./psi/gs.c:95:16 #26 0x7f1aa645b96 in __libc_start_main /build/glibc-OTsEL5/glibc- 2.27/csu/../csu/libc-start.c:310 #27 0x482e79 in _start (gs+0x482e79) 0x62a0003addf8 is located 0 bytes to the right of 23544-byte region [0x62a0003a8200,0x62a0003addf8) allocated by thread T0 here: #0 0x542d30 in __interceptor_malloc (gs+0x542d30) #1 0x23640fd in gs_heap_alloc_bytes ghostpd1/./base/gsmalloc.c:193:34 SUMMARY: AddressSanitizer: heap-buffer-overflow ghostpd1/./contrib/lips4/gdevlips.c:148:23 in GetNumSameData Shadow bytes around the buggy address: 0x0c548006db60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0x0c548006db70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0x0c548006db80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0x0c548006db90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0x0c548006dba0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 =>0x0c548006dbb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa] 0x0c548006dbc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c548006dbd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c548006dbe0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c548006dbf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c548006dc00: 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: fe 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
==9464==ABORTING
```

Julian Smith 2019-10-30 09:49:27 UTC

[Comment 1](#)

Fixed in: <https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=9f39ed4a92578a020ae10459643e1fe72573d134>