

New issue

Jump to bottom

# Multiple crashes when converting png files #73

 Closed hongxuchen opened this issue on Jul 28, 2018 · 1 comment

Assignees



Labels

bug

hongxuchen commented on Jul 28, 2018

Our fuzzer detected several crashes when converting png files against [2df6437](#) (compiled with Address Sanitizer). The command to trigger that is `img2sixel $POC -o /tmp/test.six` where \$POC can be:

heap-buffer-overflow

[https://github.com/ntu-sec/pocs/blob/master/libsixel-2df6437/crashes/hbo\\_dither.c%3A656\\_1.png](https://github.com/ntu-sec/pocs/blob/master/libsixel-2df6437/crashes/hbo_dither.c%3A656_1.png)

[https://github.com/ntu-sec/pocs/blob/master/libsixel-2df6437/crashes/hbo\\_dither.c%3A656\\_2.png](https://github.com/ntu-sec/pocs/blob/master/libsixel-2df6437/crashes/hbo_dither.c%3A656_2.png)

gdb output is like:

```
GNU gdb (Ubuntu 8.1-0ubuntu3) 8.1.0.20180409-git
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /home/hongxu/FOT/libsixel/install/bin/img2sixel...done.
Starting program: /home/hongxu/FOT/libsixel/install/bin/img2sixel hbo_dither.c:656_1.png -o /tmp/test.six
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
paletted PNG(PNG_COLOR_TYPE_PALETTE)
palette colors: 1
bitdepth: 8
=====
==16702==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000004df3 at pc 0x7fffffa5d0 sp 0x7fffff9d80
READ of size 6 at 0x602000004df3 thread T0
#0 0x4d8fb1 in __asan_memcpy (/home/hongxu/FOT/libsixel/install/bin/img2sixel+0x4d8fb1)
#1 0x7ffff7afed6c in sixel_dither_set_palette /home/hongxu/FOT/libsixel/src/dither.c:656:5
#2 0x7ffff7b6c4a8 in sixel_encoder_prepare_palette /home/hongxu/FOT/libsixel/src/encoder.c:526:9
#3 0x7ffff7b6af5 in sixel_encoder_encode_frame /home/hongxu/FOT/libsixel/src/encoder.c:975:14
#4 0x7ffff7b6a0bb in load_image_callback /home/hongxu/FOT/libsixel/src/encoder.c:1673:12
#5 0x7ffff7b1795 in load_with_builtin /home/hongxu/FOT/libsixel/src/loader.c:913:14
#6 0x7ffff7b10116 in sixel_helper_load_image_file /home/hongxu/FOT/libsixel/src/loader.c:1352:18
#7 0x7ffff7b69d98 in sixel_encoder_encode /home/hongxu/FOT/libsixel/src/encoder.c:1737:14
#8 0x515787 in main /home/hongxu/FOT/libsixel/converters/img2sixel.c:457:22
#9 0x7ffff61a6b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
#10 0x41a239 in _start (/home/hongxu/FOT/libsixel/install/bin/img2sixel+0x41a239)

0x602000004df3 is located 0 bytes to the right of 3-byte region [0x602000004df0,0x602000004df3)
allocated by thread T0 here:
#0 0x4da0f0 in __interceptor_malloc (/home/hongxu/FOT/libsixel/install/bin/img2sixel+0x4da0f0)
#1 0x7ffff7b2599 in sixel_allocator_malloc /home/hongxu/FOT/libsixel/src/allocator.c:150:12
#2 0x7ffff7b54b02 in load_png /home/hongxu/FOT/libsixel/src/loader.c:414:46
#3 0x7ffff7b10f54 in load_with_builtin /home/hongxu/FOT/libsixel/src/loader.c:839:18
#4 0x7ffff7b10116 in sixel_helper_load_image_file /home/hongxu/FOT/libsixel/src/loader.c:1352:18
#5 0x7ffff7b69d98 in sixel_encoder_encode /home/hongxu/FOT/libsixel/src/encoder.c:1737:14
#6 0x515787 in main /home/hongxu/FOT/libsixel/converters/img2sixel.c:457:22
#7 0x7ffff61a6b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/hongxu/FOT/libsixel/install/bin/img2sixel+0x4d8fb1) in __asan_memcpy
Shadow bytes around the buggy address:
0x0c047fff8960: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fff8970: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fff8980: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fff8990: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fff89a0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
=>0x0c047fff89b0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa[03]fa
0x0c047fff89c0: fa fa fd fa fa fa fd fd fa fa fa fa fa fa fa fa
0x0c047fff89d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff89e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff89f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8a00: 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
==16702==ABORTING

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
#0  __GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff61c5801 in __GI_abort () at abort.c:79
#2  0x00000000050376b in __sanitizer::Abort() ()
#3  0x000000000500a98 in __sanitizer::Die() ()
#4  0x0000000004e2d1d in __asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool, unsigned long, unsigned int, bool) ()
#5  0x0000000004d8fd1 in __asan_memcpy ()
#6  0x00007ffff7afed6d in sixel_dither_set_palette (dither=0x608000000220, palette=0x602000004df0 "\347\350", <incomplete sequence \345>) at dither.c:656
#7  0x00007ffff7b6c4a9 in sixel_encoder_prepare_palette (encoder=0x610000000040, frame=0x607000000020, dither=0x7fffff7fa940) at encoder.c:526
#8  0x00007ffff7b6a6f6 in sixel_encoder_encode_frame (encoder=0x610000000040, frame=0x607000000020, output=0x0) at encoder.c:975
#9  0x00007ffff7b6a0bc in load_image_callback (frame=0x607000000020, data=0x610000000040) at encoder.c:1673
#10 0x00007ffff7b11796 in load_with_builtin (pchunk=0x603000000e20, fstatic=0x0, fuse_palette=0x1, reqcolors=0x100, bgcolor=0x0, loop_control=0x0, fn_load=0x7ffff7b6a090
<load_image_callback>, context=0x610000000040) at loader.c:913
#11 0x00007ffff7b10117 in sixel_helper_load_image_file (filename=0x7fffff7fc9ee "hbo_dither.c:656_1.png", fstatic=0x0, fuse_palette=0x1, reqcolors=0x100, bgcolor=0x0,
loop_control=0x0, fn_load=0x7ffff7b6a090 <load_image_callback>, finsecure=0x0, cancel_flag=0x13b61c0 <signaled>, context=0x610000000040, allocator=0x604000000190) at loader.c:1352
#12 0x00007ffff7b69d99 in sixel_encoder_encode (encoder=0x610000000040, filename=0x7fffff7fc9ee "hbo_dither.c:656_1.png") at encoder.c:1737
#13 0x000000000515788 in main (argc=0x4, argv=0x7fffff7fc488) at img2sixel.c:457

```

two aborts (linked with libpng16, there is a similar issue as observed in [FLUF-hub/FLUF#515](#))

[https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt\\_loader.c%3A312\\_1.png](https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt_loader.c%3A312_1.png)  
[https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt\\_loader.c%3A312\\_2.png](https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt_loader.c%3A312_2.png)  
[https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt\\_loader.c%3A581\\_1.png](https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt_loader.c%3A581_1.png)  
[https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt\\_loader.c%3A581\\_2.png](https://github.com/ntu-sec/pocs/blob/master/libisixel-2df6437/crashes/sigabrt_loader.c%3A581_2.png)

gdb outputs are like:

```

GNU gdb (Ubuntu 8.1-0ubuntu3) 8.1.0.20180409-git
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /home/hongxu/FOT/libisixel/install/bin/img2sixel...done.
Starting program: /home/hongxu/FOT/libisixel/install/bin/img2sixel sigabrt_loader.c:312_1.png -o /tmp/test.six
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
libpng error: IHDR: CRC error

```

```

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
#0  __GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff61c5801 in __GI_abort () at abort.c:79
#2  0x00007ffff7247618 in png_longjmp () from /usr/lib/x86_64-linux-gnu/libpng16.so.16
#3  0x00007ffff7247687 in png_error () from /usr/lib/x86_64-linux-gnu/libpng16.so.16
#4  0x00007ffff7247710 in png_chunk_error () from /usr/lib/x86_64-linux-gnu/libpng16.so.16
#5  0x00007ffff7255cfd in ?? () from /usr/lib/x86_64-linux-gnu/libpng16.so.16
#6  0x00007ffff725641e in ?? () from /usr/lib/x86_64-linux-gnu/libpng16.so.16
#7  0x00007ffff724c57e in png_read_info () from /usr/lib/x86_64-linux-gnu/libpng16.so.16
#8  0x00007ffff7b52f4c in load_png (result=0x607000000020, buffer=0x62d0000000400 "\211PNG\r\n\032\n", size=0x125, psx=0x607000000038, psy=0x60700000003c, ppalette=0x607000000030,
pncolors=0x607000000040, reqcolors=0x100, pixelformat=0x607000000044, bgcolor=0x0, transparent=0x607000000058, allocator=0x604000000190) at loader.c:312
#9  0x00007ffff7b10f55 in load_with_builtin (pchunk=0x603000000e20, fstatic=0x0, fuse_palette=0x1, reqcolors=0x100, bgcolor=0x0, loop_control=0x0, fn_load=0x7ffff7b6a090
<load_image_callback>, context=0x610000000040) at loader.c:839
#10 0x00007ffff7b10117 in sixel_helper_load_image_file (filename=0x7fffff7fc9ea "sigabrt_loader.c:312_1.png", fstatic=0x0, fuse_palette=0x1, reqcolors=0x100, bgcolor=0x0,
loop_control=0x0, fn_load=0x7ffff7b6a090 <load_image_callback>, finsecure=0x0, cancel_flag=0x13b61c0 <signaled>, context=0x610000000040, allocator=0x604000000190) at loader.c:1352
#11 0x00007ffff7b69d99 in sixel_encoder_encode (encoder=0x610000000040, filename=0x7fffff7fc9ea "sigabrt_loader.c:312_1.png") at encoder.c:1737
#12 0x000000000515788 in main (argc=0x4, argv=0x7fffff7fc488) at img2sixel.c:457

```

Other system information:


```


# Ubuntu 18.04 x86_64
$ ldd ~/FOT/libisixel-fuzz/install/bin/img2sixel
linux-vdso.so.1 (0x00007ffe38544000)
libisixel.so.1 => /home/hongxu/FOT/libisixel-fuzz/install/lib/libisixel.so.1 (0x00007ff2905c6000)
libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007ff290228000)
libcurl-gnutls.so.4 => /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4 (0x00007ff28ffab000)
libpng16.so.16 => /usr/lib/x86_64-linux-gnu/libpng16.so.16 (0x00007ff28fd79000)
libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007ff28fb5c000)
libjpeg.so.8 => /usr/lib/x86_64-linux-gnu/libjpeg.so.8 (0x00007ff28f8f4000)
libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007ff28fd5000)
librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007ff28f4cd000)
libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007ff28f2c9000)
libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007ff28f0b1000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007ff28ecc0000)
/lib64/ld-linux-x86-64.so.2 (0x00007ff290a22000)
libnghttp2.so.14 => /usr/lib/x86_64-linux-gnu/libnghttp2.so.14 (0x00007ff28ea9b000)
libidn2.so.0 => /usr/lib/x86_64-linux-gnu/libidn2.so.0 (0x00007ff28e87e000)
librtmp.so.1 => /usr/lib/x86_64-linux-gnu/librtmp.so.1 (0x00007ff28e662000)
libpsl.so.5 => /usr/lib/x86_64-linux-gnu/libpsl.so.5 (0x00007ff28e454000)
libnettle.so.6 => /usr/lib/x86_64-linux-gnu/libnettle.so.6 (0x00007ff28e21e000)
libgnutls.so.30 => /usr/lib/x86_64-linux-gnu/libgnutls.so.30 (0x00007ff28deb9000)
libgssapi_krb5.so.2 => /usr/lib/x86_64-linux-gnu/libgssapi_krb5.so.2 (0x00007ff28dc6e000)
libldap_r-2.4.so.2 => /usr/lib/x86_64-linux-gnu/libldap_r-2.4.so.2 (0x00007ff28da1c000)
liblber-2.4.so.2 => /usr/lib/x86_64-linux-gnu/liblber-2.4.so.2 (0x00007ff28d80e000)
libunistring.so.2 => /usr/lib/x86_64-linux-gnu/libunistring.so.2 (0x00007ff28d490000)
libhogweed.so.4 => /usr/lib/x86_64-linux-gnu/libhogweed.so.4 (0x00007ff28d25c000)
libgmp.so.10 => /usr/lib/x86_64-linux-gnu/libgmp.so.10 (0x00007ff28cdfb000)
libp11-kit.so.0 => /usr/lib/x86_64-linux-gnu/libp11-kit.so.0 (0x00007ff28ccac000)
libtasn1.so.6 => /usr/lib/x86_64-linux-gnu/libtasn1.so.6 (0x00007ff28ca99000)
libkrb5.so.3 => /usr/lib/x86_64-linux-gnu/libkrb5.so.3 (0x00007ff28c7c3000)
libk5crypto.so.3 => /usr/lib/x86_64-linux-gnu/libk5crypto.so.3 (0x00007ff28c591000)
libcom_err.so.2 => /lib/x86_64-linux-gnu/libcom_err.so.2 (0x00007ff28c38d000)
libkrb5support.so.0 => /usr/lib/x86_64-linux-gnu/libkrb5support.so.0 (0x00007ff28c182000)
libresolv.so.2 => /lib/x86_64-linux-gnu/libresolv.so.2 (0x00007ff28bf67000)

```


```
libssl.so.2 => /usr/lib/x86_64-linux-gnu/libssl.so.2 (0x00007ff28bd4c000)
libgssapi.so.3 => /usr/lib/x86_64-linux-gnu/libgssapi.so.3 (0x00007ff28bb0b000)
libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007ff28b903000)
libkeyutils.so.1 => /lib/x86_64-linux-gnu/libkeyutils.so.1 (0x00007ff28b6ff000)
libheimtlib.so.0 => /usr/lib/x86_64-linux-gnu/libheimtlib.so.0 (0x00007ff28b4f6000)
libkrb5.so.26 => /usr/lib/x86_64-linux-gnu/libkrb5.so.26 (0x00007ff28b269000)
libasn1.so.8 => /usr/lib/x86_64-linux-gnu/libasn1.so.8 (0x00007ff28afc7000)
libhcrypto.so.4 => /usr/lib/x86_64-linux-gnu/libhcrypto.so.4 (0x00007ff28ad91000)
libroken.so.18 => /usr/lib/x86_64-linux-gnu/libroken.so.18 (0x00007ff28ab7b000)
libwind.so.0 => /usr/lib/x86_64-linux-gnu/libwind.so.0 (0x00007ff28a952000)
libheimbase.so.1 => /usr/lib/x86_64-linux-gnu/libheimbase.so.1 (0x00007ff28a743000)
libhx509.so.5 => /usr/lib/x86_64-linux-gnu/libhx509.so.5 (0x00007ff28a4f9000)
libsqlite3.so.0 => /usr/lib/x86_64-linux-gnu/libsqlite3.so.0 (0x00007ff28a1f0000)
libcrypt.so.1 => /lib/x86_64-linux-gnu/libcrypt.so.1 (0x00007ff289fb8000)
```

 **saitoha** self-assigned this on Aug 2, 2018

 **saitoha** added a commit that referenced this issue on Dec 15, 2019


 Avoid illegal memory access problem with 1 color paletted png([#73](#)), ...

cb373ab

 **saitoha** added a commit that referenced this issue on Dec 15, 2019

 Handle libpng error message ([#73](#)), thanks to HongxuChen

26ac06f

 **saitoha** added the `bug` label on Dec 15, 2019

**saitoha** commented on Dec 18, 2019

Owner

Fixed on [v1.8.4](#). Thanks!

 **saitoha** closed this as completed on Dec 18, 2019

#### Assignees

 **saitoha**

#### Labels

bug

#### Projects

None yet

#### Milestone

No milestone

#### Development

No branches or pull requests

#### 2 participants