New issue

Jump to bottom

FPE in sixel_encoder_do_resize, encoder.c:633 #166

Open waugustus opened this issue on Apr 25 · 4 comments

waugustus commented on Apr 25 • edited

Description

There is a floating point exception error in sixel_encoder_do_resize, encoder.c:633 in img2sixel 1.8.6. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted JPEG file.

Version

img2sixel 1.8.6, commit id `6a5be8b` (Tue Jan 14 02:27:00 2020 +0900)

Reproduction

```
# img2sixel -w 128 poc /tmp/foo
ASAN:DEADLYSIGNAL
=================================================================
==1596536==ERROR: AddressSanitizer: FPE on unknown address 0x55718c759aa0 (pc 0x55718c759aa0 bp
0x7fff1eb09d20 sp 0x7fff1eb09cf0 T0)
    #0 0x55718c759a9f in sixel_encoder_do_resize /root/programs/libsixel/src/encoder.c:633
    #1 0x55718c75b5e5 in sixel_encoder_encode_frame /root/programs/libsixel/src/encoder.c:968
    #2 0x55718c760d75 in load_image_callback /root/programs/libsixel/src/encoder.c:1679
    #3 0x55718c7c883d in load_gif /root/programs/libsixel/src/fromgif.c:671
    #4 0x55718c7c0d74 in load_with_builtin /root/programs/libsixel/src/loader.c:908
    #5 0x55718c7c19cb in sixel_helper_load_image_file /root/programs/libsixel/src/loader.c:1418
    #6 0x55718c7612e7 in sixel_encoder_encode /root/programs/libsixel/src/encoder.c:1743
    #7 0x55718c7549ee in main /root/programs/libsixel/converters/img2sixel.c:457
    #8 0x7f382df64c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #9 0x55718c752109 in _start (/root/programs/libsixel/build_asan/bin/img2sixel+0x5e109)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /root/programs/libsixel/src/encoder.c:633 in
sixel_encoder_do_resize
==1596536==ABORTING
```

poc.zip

Platform

```
# uname -a
Linux 4a409ce47130 5.4.0-70-generic #78~18.04.1-Ubuntu SMP Sat Mar 20 14:10:07 UTC 2021 x86_64
x86_64 x86_64 GNU/Linux
```

carnil commented on May 12

Can you report the issue to the new upstream at https://github.com/libsixel/libsixel ?

carnil commented on May 12

Maybe this project should as well be archived if it's not anymore the main upstream repository for libsixel.

waugustus mentioned this issue on May 12

FPE in sixel_encoder_do_resize, encoder.c:610 libsixel/libsixel#63

Open

waugustus commented on May 12 — Author

> Can you report the issue to the new upstream at https://github.com/libsixel/libsixel ?

OK, and thank you for your suggestion.

waugustus commented on May 17 — Author

CVE-2022-29978 assigned.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants