New issue

Jump to bottom

Assertion failure in stbi__jpeg_huff_decode, stb_image.h:1894 #165

Open **waugustus** opened this issue on Apr 23 · 3 comments

waugustus commented on Apr 23 • edited

Description

There is an assertion failure error in stbi__jpeg_huff_decode, stb_image.h:1894. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted jpg file.

Version

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

Reproduction

```
# img2sixel poc -o /tmp/foo
img2sixel: stb_image.h:1894: stbi__jpeg_huff_decode: Assertion `(((j->code_buffer) >> (32 - h->size[c])) & stbi__bmask[h->size[c]]) == h->code[c]' failed.
Aborted (core dumped)
```

poc.zip

Platfrom

```
# 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 ?

waugustus mentioned this issue on May 12

Assertion failure in stbi__jpeg_huff_decode, stb_image.h:2115 libsixel/libsixel#62

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-2022-29977 assigned.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants