


New issue

Jump to bottom

Floating point exception #66

 Closed strongcourage opened this issue on Jul 18, 2019 · 2 comments

strongcourage commented on Jul 18, 2019

Hi,

I found a FPE bug on the latest commit `cafd4b8` of master.

PoC: https://github.com/strongcourage/PoCs/blob/master/sam2p_cafd4b8/PoC_fpe
Command: `sam2p $PoC /tmp/out.bmp`

ASAN says:


```
This is sam2p 0.49.4.  
Available Loaders: PS PDF JAI PNG JPEG TIFF PNM BMP GIF LBM XPM PCX TGA.  
Available Appliers: XWD Meta Empty BMP PNG TIFF6 TIFF6-JAI JPEG-JAI JPEG PNM GIF89a+LZW XPM PSL1C PSL23+PDF PSL2+PDF-JAI P-TrOpBb.  
sam2p-asan: Warning: TGA: 24 bit image, 9 bit alpha is greater than 24 total bits per pixel  
sam2p-asan: Warning: TGA: reducing to * bit alpha: 0  
Floating point exception
```


Thanks,
Manh Dung


 pts closed this as completed in [b953f63](#) on Jul 18, 2019

pts commented on Jul 18, 2019 Owner

Thank you for reporting this! Fixed in [b953f63](#) .

The new behavior is failing with a more informative error message:


```
sam2p: Error: Image: Image of size 0.
```


 1

fgeek commented on Jul 27, 2021

[CVE-2020-19492](#) has been assigned for this issue.

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants

