New issue

Jump to bottom

# SEGV in CGIF::AddExtensionBlock (cgif.c:470) #67

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

**strongcourage** commented on Jul 18, 2019

Hi,

I found a crash in the function CGIF::AddExtensionBlock on the latest commit `cafd4b8` of master. It seems that it is due to an incomplete patch of #36.

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

ASAN says:

```
==29941==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000030 (pc 0x000000428586 bp 0x7fff8308aaa0 sp 0x7fff8308aa70 T0)
    #0 0x428585 in CGIF::AddExtensionBlock(CGIF::SavedImage*, int, unsigned char*) /home/dungnguyen/gueb-testing/sam2p/cgif.c:470
    #1 0x42e9df in CGIF::DGifSlurp(CGIF::GifFileType*) /home/dungnguyen/gueb-testing/sam2p/cgif.c:1554
    #2 0x42ec04 in in_gif_reader /home/dungnguyen/gueb-testing/sam2p/in_gif.cpp:60
    #3 0x491694 in Image::load(Image::Loader::UFD*, SimBuffer::Flat const&, char const*) /home/dungnguyen/gueb-testing/sam2p/image.cpp:1435
    #4 0x4095f3 in run_sam2p_engine(Files::FILEW&, Files::FILEW&, char const* const*, unsigned char) /home/dungnguyen/gueb-testing/sam2p/sam2p_main.cpp:1055
    #5 0x40a73e in main /home/dungnguyen/gueb-testing/sam2p/sam2p_main.cpp:1148
    #6 0x7f4e3c42082f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #7 0x401fa8 in _start (/home/dungnguyen/PoCs/sam2p_cafd4b8/sam2p-asan+0x401fa8)
```

Thanks,
Manh Dung

**pts** closed this as completed in `1d62cf8` on Jul 18, 2019

**pts** commented on Jul 18, 2019 Owner

Thank you for reporting this! Fixed in `1d62cf8` .

**fgeek** commented on Jul 27, 2021

CVE-2020-19491 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