Closed · Issue created 1 year ago by 5n1p3r0010

[Security]Heap-buffer-overflow issue with djxl decode routine

This is the copy of confidential issue-159,since the matainer said it has been fixed in their 'internal master branch',I make it public it here.

There is a heap buffer overflow issue with jpeg-xl decode routine,this can reproduce on the lattest commit,aka:`5175d117`.

Steps to reproduce:

The flags and compiler I use was:

mkdir asan

cd asan

cmake .. -DCMAKE_C_COMPILER=clang -DCMAKE_CXX_COMPILER=clang++ -DCMAKE_C_FLAGS="-fsanitize=address" -DCMAKE_CXX_FLAGS="-fsanitize=address"

make

Or just build without asan was OKAY. Run as: /path/to/djxl /path/to/poc ./t.png

What went wrong:

The djxl build with asan shows follow:

Read 1103 compressed bytes [v0.3.2 | SIMD supported: AVX2,SSE4,Scalar]

==729079==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x629000004a00 at pc 0x55a7acd8e9ed bp 0x7fff875a8430 sp 0x7fff875a8428

Reporter:

5n1p3r0010 from Topsec Alpha Lab

heap-buffer-overflow1

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related. Learn more.

Activity

Jon Sneyers added decoder bug fixed labels 1 year ago

Jyrki Alakuijala assigned to @eustas 1 year ago

Jyrki Alakuijala @jyrkialakuijala · 1 year ago — Maintainer
Eugene, could you verify this.

Eugene Kliuchnikov @eustas · 1 year ago — Maintainer
Done. Does not reproduce on ToT build.

Eugene Kliuchnikov @eustas · 1 year ago — Maintainer
(Will check with 0.3.3 or next tag later)

Eugene Kliuchnikov @eustas · 1 year ago — Maintainer
There is commit after 0.3.2 where it reproduces. Does not reproduce in 0.3.3 -> fixed.

Eugene Kliuchnikov closed 1 year ago

Please register or sign in to reply