[BUG] Reachable assertion in inttobits, jas_image.c #338

Closed kdsjZh opened this issue on Sep 13 · 10 comments

kdsjZh commented on Sep 13 • edited

summary

Hello, I was testing my fuzzer and found a reachable assertion in imginfo. An assertion in function inttobits can be reached when parsing a crafted jp2 file, when running `./imginfo -f $POC`, as shown in the attachment

Environment

- Ubuntu 22.04 (docker)
- gcc/g++ 11.2.0
- jasper latest commit `0c2a927`

Step to reproduce

```
mkdir jasper-build && pushd jasper-build
cmake -DJAS_ENABLE_SHARED=NO .. && make -j$(nproc)
./src/app/imginfo -f $POC
```

output

```
imginfo: /benchmark/jasper/src/libjasper/base/jas_image.c:1010: inttobits: Assertion `v >= 0 ||
sgnd' failed.
Aborted (core dumped)
```

POC

poc0.zip

Credit

Han Zheng (NCNIPC of China, Hexhive)
Yin Li, Xiaotong Jiao (NCNIPC of China)

jubalh commented on Sep 19 — Member

It seems like this issue got assigned CVE-2022-40755.
@kdsjZh do I see it right that no release is vulnerable to this only master?

kdsjZh commented on Sep 19 — Author

I only tested with the master commit so I'm not sure if it can occur in the previous release. I tried with previous release and the poc cannot triggered the expected behavior, but it doesn't mean previous release is not vulnerable. I could try to fuzz previous release to see if previous releases are affected but fixing it directly might be the simplest solution

jubalh commented on Sep 19 — Member

> but fixing it directly might be the simplest solution

sure. I was just curious about the CVE state.

@mdadams we should also include this in 3.0.7.

kdsjZh commented on Sep 19 — Author

Ok, then I'll start testing the latest release. I'll let you know if we got the poc.

👍 1

kdsjZh commented on Sep 22 — Author

I tried the latest release these days and didn't find it. According to my experience this assertion is not reachable (or at least not easy to reach) in the latest release. Considering I've fuzzed it for about 3 days without any finding and it takes only 12h to find it in the latest commit, I would say that only master is vulnerable.

jubalh commented on Sep 22 — Member

@kdsjZh thanks for checking this.

mdadams commented 22 days ago — Collaborator

This appears to be a duplicate of the bug #345 fixed in commit `34faad5` . I no longer have this problem as of the most recent commit on the master branch. So, I am going to close this issue. If you continue to have problems, please let me know.

 **mdadams** closed this as completed 22 days ago

---

theta682 commented 22 days ago — Contributor

@mdadams can you release a new version with this fix?

mdadams commented 22 days ago — Collaborator

The CI testing is failing for Ubuntu with Clang. This is under invesitgation at the moment. It would not be wise to make a new release until reason for this failure has been isolated because if this is not a benign problem it will potentially impact many users.

jubalh commented 22 days ago — Member

Hmm I see:

```
Test project /home/runner/work/jasper/jasper/tmp_cmake/shared_release-0/build
    Start 1: run_test_imginfo
1/5 Test #1: run_test_imginfo ................***Failed    0.75 sec
JPG: 1
MIF: 0
SKIPPING: unsupported format (mif)
jas_image_decode: decode operation failed
cannot load image
imginfo failed for images/feep2.pnm (1)
```

etc at https://github.com/jasper-software/jasper/actions/runs/3390689264/jobs/5635106290#step:4:5903

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants