


New issue

Jump to bottom

jp2_decode() Null Pointer Access #265

 Closed dgh05t opened this issue on Jan 29, 2021 · 3 comments

dgh05t commented on Jan 29, 2021

Hi,
There's a Null Pointer Access in `jp2_decode` `/home/dgh05t/fuzz/jasper-master/src/libjasper/jp2/jp2_dec.c:442`
run the poc with `"./jasper -f ~/Desktop/poc2.jp2 --output-format jpg"`
poc:
[poc2.zip](#)

thoger commented on Jan 29, 2021


Contributor

It crashes here:
https://github.com/jasper-software/jasper/blob/version-2.0.24/src/libjasper/jp2/jp2_dec.c#L434
It happens on attempt to access `dec->image->cmts[3]`, while `dec->image->numcmts_` is 3.
Note that the first version that crashes with this reproducer is 2.0.20, and bisecting changes since 2.0.19 found [a4dc77c](#) as the first affected. It's not immediately obvious if that commit introduces the issue, or if it only makes it it reachable for a particular reproducer.

mdadams commented on Feb 7, 2021



Collaborator

@dgh05t @thoger This problem appears to be resolved by the fix for [#264](#). Please give version-2.0.25 a try. If this does not fix the problem for you, let me know, and I can reopen the issue. Incidentally, I added the JP2 files for [#264](#) and [#265](#) to the test suite (as `poc_264.jp2` and `poc_265.jp2`).


 mdadams closed this as completed on Feb 7, 2021


utkarsh2102 commented on Feb 10, 2021

CVE-2021-26927 has been assigned for this issue.


  theta682 mentioned this issue on Mar 1, 2021

jp2_decode() heap-buffer-overflow vulnerability #264




 This was referenced on Mar 22, 2021

A null pointer dereference in jp2_decode in jp2_dec.c #269



A Null Pointer dereference #268



Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

4 participants

