CVE-2022-2831 - Blender issue #99705: Out-of-bounds memory access due to blender-thumbnailer

Local preservation snapshot
Source: https://projects.blender.org/blender/blender/issues/99705
Retrieved: 2026-11-17 11:54:18 KST
Capture method: Official Blender issue API content typeset to PDF

This PDF is a local archival copy. The original vendor page remains the authoritative source.

State	Created	Updated
closed	2022-07-14T17:46:21+02:00	2023-02-10T13:03:22+01:00

Issue report

System Information

Operating system: Ubuntu 20.04.4 LTS Graphics card: 2b:00.0 VGA compatible controller: NVIDIA Corporation TU116 [GeForce GTX 1650 SUPER] (rev a1)

Blender Version

Broken: Blender 3.3.0 Alpha branch : master, commit c8a07ef66311a31cc45901717845139ae0682f2f commit Date: Thu Jul 14 11:32:01 2022 +0200

Short description of error

A loaded (and valid) image can be crafted such that an out-of-bounds read or write occurs when the image converted to thumbnail that is flipped vertically. Crash occured in

```
that include memcpy()



**Exact steps for others to reproduce the error**
Based on the default startup or an attached .blend file (as simple as possible).


**Impact**
An attacker-controlled out-of-bounds write/read can trigger code execution through convert this .blender file to thumbnail imag

[crash_final.blender](https://archive.blender.org/developer/F13292704/crash_final.blender)

POC Videos is below
https://youtu.be/WN2t86t6m6k

POC blender file is below
https://drive.google.com/file/d/1pWe-t4LuirvgSdVaaaS1dle1trNWGPiw/view?usp=sharing
```

Discussion history (10 comments)

sangjun-park - 2022-07-14T17:46:21+02:00

Added subscriber: @sangjun-park

sangjun-park - 2022-07-14T18:02:01+02:00

Sorry for my mistake.

the crash_final.blender that i include to show proof of concept need to change extension name that .blend

but it doesn't matter extesion that reproduce Crash

but change file name

rjg - 2022-07-14T18:40:25+02:00

Added subscriber: @rjg

LazyDodo - 2022-07-14T18:55:24+02:00

Changed status from 'Needs Triage' to: 'Confirmed'

LazyDodo - 2022-07-14T20:18:07+02:00

Changed status from 'Confirmed' to: 'Resolved'

blender-admin - 2022-07-14T20:18:35+02:00

This issue was referenced by 32df09b2416a6961704eca0fe73534c8c4e715b2

blender-admin - 2022-07-14T20:18:35+02:00

This issue was referenced by b1329d7eaa52a11c73b75d19d20bd8f6d11ac535

sangjun-park - 2022-07-14T20:37:03+02:00

Added subscriber: @LazyDodo

sangjun-park - 2022-07-14T20:37:03+02:00

It's amazing that they patched it so quickly.

Thanks.

Can i apply for a CVE number at https://cveform.mitre.org/ ???

LazyDodo - 2022-07-14T20:45:26+02:00

I'm not involved with mitre, so i couldn't tell you about their process. Community wise however if you're clever enough to find this kind of bug, you surely can provide a patch to fix it which actually would make blender better. Something to keep in mind for future reports.