

Out-of-bounds memory access due to blender-thumbailer

Closed, Resolved Public

Actions

Assigned To

None

Authored By

Sangjun Park (Sangjun)

Jul 14 2022, 5:46 PM

Tags

BF Blender (Backlog)

Subscribers

Ray molenkamp (LazyDodo)

Robert Guetzkow (rjg)

Sangjun Park (Sangjun)

Description

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 occurred in

```
source/blender/blendthumb/src/blendthumb_extract.cc
```

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 image using blender-thumbailer



crash_final.blender 140 B

Download

POC Videos is below

<https://youtu.be/WN2t86t6m6k>

POC blender file is below

<https://drive.google.com/file/d/1pWe-t4LuirvgSdVaaaS1dle1trNWGPiw/view?usp=sharing>

Revisions and Commits

rB Blender

rB32df09b2416a **Fix T99705: fix integer overflow in thumbnail extractor**

rBb1329d7eaa52 **Fix T99705: fix integer overflow in thumbnail extractor**

Related Objects

Mentions

Mentioned In

~~T98661: 3.2: Potential candidates for corrective releases~~

[T88449: Blender LTS: Maintenance Task 2.93](#)

Mentioned Here

[rBc8a07ef66311: BLI: fix finding indices from virtual array](#)

Sangjun Park (Sangjun) created this task. Jul 14 2022, 5:46 PM

Sangjun Park (Sangjun) added a comment. Jul 14 2022, 6:02 PM

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

crash_final.blender ---> crash_final.blend

Robert Guetzkow (rjg) added a subscriber: **Robert Guetzkow (rjg)**. Jul 14 2022, 6:40 PM

-  **Ray molenkamp (LazyDodo)** changed the task status from *Needs Triage* to *Confirmed*. Jul 14 2022, 6:55 PM
-  **Ray molenkamp (LazyDodo)** claimed this task.
-  **Ray molenkamp (LazyDodo)** added a revision: ~~D15457: Fix T99705: fix integer overflow in thumbnail extractor.~~
-  **Ray molenkamp (LazyDodo)** closed this task as *Resolved* by committing **rBb1329d7eaa52: Fix T99705: fix integer overflow in thumbnail extractor.** Jul 14 2022, 8:18 PM
-  **Ray molenkamp (LazyDodo)** added a commit: **rBb1329d7eaa52: Fix T99705: fix integer overflow in thumbnail extractor.**
-  **Ray molenkamp (LazyDodo)** mentioned this in **T88449: Blender LTS: Maintenance Task 2.93.** Jul 14 2022, 8:22 PM
-  **Ray molenkamp (LazyDodo)** mentioned this in ~~T98661: 3.2: Potential candidates for corrective releases.~~


 **Sangjun Park (Sangjun)** removed **Ray molenkamp (LazyDodo)** as the assignee of this task. Jul 14 2022, 8:37 PM

 **Sangjun Park (Sangjun)** added a subscriber: **Ray molenkamp (LazyDodo)**.


It's amazing that they patched it so quickly.

Thanks.

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

 **Ray molenkamp (LazyDodo)** added a comment. Jul 14 2022, 8:45 PM

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.

 **Thomas Dinges (dingto)** added a commit: **rB32df09b2416a: Fix T99705: fix integer overflow in thumbnail extractor.** Jul 15 2022, 3:04 PM

[Log In to Comment](#)