

New issue

Jump to bottom

## SEGV exrmakepreview in makePreview.cpp:132 #493

 strongcourage opened this issue on Jul 24, 2019 · 6 comments

Labels Bug

strongcourage commented on Jul 24, 2019

Hi,

I found a null pointer dereference bug on exrmakepreview (the latest commit [9418823](#) on master).

PoC: [https://github.com/strongcourage/PoCs/blob/master/openexr\\_9410823/PoC\\_npd\\_generatePreview](https://github.com/strongcourage/PoCs/blob/master/openexr_9410823/PoC_npd_generatePreview)

Command: exrmakepreview -v \$PoC /dev/null

ASAN says:

```
==5549==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000402db3 bp 0x7fbf849cd800 sp 0x7ffe12fc8050 T0)
#0 0x402db2 in generatePreview /home/dungnguyen/gueb-testing/openexr/OpenEXR/exrmakepreview/makePreview.cpp:132
#1 0x402db2 in makePreview(char const*, char const*, int, float, bool) /home/dungnguyen/gueb-testing/openexr/OpenEXR/exrmakepreview/makePreview.cpp:162
#2 0x402187 in main /home/dungnguyen/gueb-testing/openexr/OpenEXR/exrmakepreview/main.cpp:185
#3 0x7fbf8244082f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#4 0x402428 in _start (/home/dungnguyen/PoCs/openexr_9410823/exrmakepreview-asan+0x402428)
```

Thanks,  
Manh Dung

 peterhillman added a commit to peterhillman/openexr that referenced this issue on Jul 25, 2019

 Fix logic for 1 pixel high/wide preview images (Fixes [AcademySoftware...](#) ...)

587ad0e

 kdt3rd closed this as completed in [7450450](#) on Jul 25, 2019

  kdt3rd added the Bug label on Jul 25, 2019

carnil commented on Dec 10, 2020

[CVE-2020-16588](#) seems to have been assigned for this issue.

theta682 commented on Dec 13, 2020

Contributor

Please, communicate with NVD (<https://nvd.nist.gov/info>) and update the applicable version. As I understand it was fixed in 2.4.0.

meshula commented on Dec 14, 2020

Contributor

@theta682 when you say communicate with NVD, do you mean send an email to the "general contact" address? I don't spot tools or instructions on their website to update the applicable version on either the info page or on the page specifically for this issue. (<https://nvd.nist.gov/vuln/detail/CVE-2020-16588>)

strongcourage commented on Dec 14, 2020

Author

Hi all,

I requested a CVE for this bugs several months ago, and recently this one has been assigned a CVE. In my report, I showed that this bug has been fixed by the developers. You can see the fix commit in the references. So I think we don't need to do anything.

Best,  
MD

meshula commented on Dec 14, 2020

Contributor

Great, thanks for looking into it!


theta682 commented on Dec 14, 2020

Contributor

@meshula on <https://nvd.nist.gov/info> you can find the e-mail ([nvd@nist.gov](mailto:nvd@nist.gov)). Previously I contacted them and they updated the CVE which I asked to update.

 1

 **DominicJacksonBFX** pushed a commit to `boris-fx/mocha-openexr` that referenced this issue on Jun 22

 Fix logic for 1 pixel high/wide preview images (Fixes [AcademySoftware...](#) ...)

781223e

Assignees

No one assigned

Labels

Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants

