

New issue

[Jump to bottom](#)

[BUG] When converting FUR to VGM with furnace console mode, there were many crashes #325

 Open

mqrsv opened this issue on Mar 29 · 5 comments

Assignees



Labels

bug critical

mqrsv commented on Mar 29

OS: ubuntu 20.04


Furnace version dev73.

Command: ./furnace -console -vgmout out.vgm poc.fur

[POC.tar.gz](#)

I use fuzz tests, so I don't analyze these crashes in detail.

I packaged the POC file so you can reproduce the error.

  freq-mod added the bug label on Mar 29

tildearrow commented on Mar 29

Owner

Also happens when opening these files... hmmm...

mqrsv commented on Mar 29

Author



I used the Fuzz tool to get hundreds of crashes in 24 hours.


Poc.tar. gz are a couple of specific errors I classified.

marcruef commented on Apr 3

FYI: This issue got [CVE-2022-1211](#) assigned (source: <https://vuldb.com/?id.196371>)


  **tildearrow** self-assigned this on Apr 4

  **tildearrow** added the **critical** label on Apr 4

 **tildearrow** added a commit that referenced this issue on Apr 4

 harden Furnace file loader ...

✓ 3a7a132

 **tildearrow** added a commit that referenced this issue on Apr 4

 harden .dmf loader ...

✓ 258a905

tildearrow commented on Apr 4

Owner

I have improved the file loader to ensure we don't go out of bounds. Please test with git master.



1

  **tildearrow** added the **feedback** label on Apr 4



 **tildearrow** closed this as completed on Apr 9


 **tildearrow** reopened this on Apr 9

tildearrow commented on Apr 9

Owner

Re-opening issue as I found one crash.

  **tildearrow** removed the **feedback** label on Apr 9

 **tildearrow** added a commit that referenced this issue on Apr 9

 fix possible pattern crash ...

✓ 0eb0242

Assignees

 **tildearrow**

Labels

bug critical

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

