☆ Starred by 1 user

Owner:	----
CC:	cbp...@gmail.com twode...@gmail.com secur...@openexr.org
Status:	Verified *(Closed)*
Components:	----
Modified:	May 8, 2021
Type:	Bug

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Stability-UndefinedBehaviorSanitizer
Engine-libfuzzer
OS-Linux
Proj-openexr
Reported-2020-10-09
Disclosure-2021-01-07

Issue 26229: openexr:openexr_scanlines_fuzzer: Undefined-shift in Imf_2_5::hufDecode

Reported by ClusterFuzz-External on Fri, Oct 9, 2020, 10:29 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=6196957322936320

Project: openexr
Fuzzing Engine: libFuzzer
Fuzz Target: openexr_scanlines_fuzzer
Job Type: libfuzzer_ubsan_openexr
Platform Id: linux

Crash Type: Undefined-shift
Crash Address:
Crash State:
  Imf_2_5::hufDecode
  Imf_2_5::hufUncompress
  Imf_2_5::PizCompressor::uncompress

Sanitizer: undefined (UBSAN)

Crash Revision: https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_openexr&revision=202009270617

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=6196957322936320

Issue filed automatically.

See https://google.github.io/oss-fuzz/advanced-topics/reproducing for instructions to reproduce this bug locally.
When you fix this bug, please
  * mention the fix revision(s).
  * state whether the bug was a short-lived regression or an old bug in any stable releases.
  * add any other useful information.
This information can help downstream consumers.

If you need to contact the OSS-Fuzz team with a question, concern, or any other feedback, please file an issue at https://github.com/google/oss-fuzz/issues. Comments on individual Monorail issues are not monitored.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse
without an upstream patch, then the bug report will automatically
become visible to the public.

Comment 1 by sheriffbot on Fri, Oct 9, 2020, 4:16 PM EDT Project Member

Labels: Disclosure-2021-01-07

Comment 2 by ClusterFuzz-External on Tue, Oct 13, 2020, 10:27 AM EDT Project Member

Status: Verified (was: New)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 6196957322936320 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_openexr&range=202010120623:202010130610

If this is incorrect, please file a bug on https://github.com/google/oss-fuzz/issues/new

Comment 3 by sheriffbot on Thu, Nov 12, 2020, 2:54 PM EST Project Member

Labels: -restrict-view-commit

This bug has been fixed for 30 days. It has been opened to the public.

- Your friendly Sheriffbot

Comment 4 by cbp...@gmail.com on Sat, May 8, 2021, 8:39 PM EDT

Fixed in v2.5.4 and beyond.
https://github.com/AcademySoftwareFoundation/openexr/pull/849