Starred by 1 user

Owner: ----

CC: kevin...@github.com
pipon...@gmail.com

Status: Verified *(Closed)*

Components: ----

Modified: Oct 23, 2022

Type: Bug

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Engine-honggfuzz
Proj-exiv2
Reported-2022-10-13
Disclosure-2023-01-11

Issue 52382: exiv2:fuzz-read-print-write: Null-dereference READ in Exiv2::QuickTimeVideo::userDataDecoder

Reported by ClusterFuzz-External on Thu, Oct 13, 2022, 2:47 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5921230406680576

Project: exiv2
Fuzzing Engine: honggfuzz
Fuzz Target: fuzz-read-print-write
Job Type: honggfuzz_asan_exiv2
Platform Id: linux

Crash Type: Null-dereference READ
Crash Address: 0x000000000008
Crash State:
  Exiv2::QuickTimeVideo::userDataDecoder
  Exiv2::QuickTimeVideo::tagDecoder
  Exiv2::QuickTimeVideo::decodeBlock

Sanitizer: address (ASAN)

Regressed: https://oss-fuzz.com/revisions?job=honggfuzz_asan_exiv2&range=202208240610:202208250610

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5921230406680576

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 Thu, Oct 13, 2022, 2:49 PM EDT Project Member

Labels: Disclosure-2023-01-11

Comment 2 by ClusterFuzz-External on Sun, Oct 23, 2022, 10:36 AM EDT Project Member

Status: Verified (was: New)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5921230406680576 is verified as fixed in https://oss-fuzz.com/revisions?job=honggfuzz_asan_exiv2&range=202210220603:202210230611

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

Comment 3 by sheriffbot on Sun, Oct 23, 2022, 2:42 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed. It has been opened to the public.

- Your friendly Sheriffbot