Starred by 1 user

Owner: ----

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

Status: Verified *(Closed)*

Components: ----

Modified: Sep 22, 2022

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Security_Severity-High
Engine-honggfuzz
Proj-exiv2
Reported-2022-09-02
Disclosure-2022-12-01

Issue 50901: exiv2:fuzz-read-print-write: Heap-buffer-overflow in Exiv2::MemIo::read

Reported by ClusterFuzz-External on Fri, Sep 2, 2022, 9:02 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5744443654799360

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

Crash Type: Heap-buffer-overflow WRITE 8
Crash Address: 0x602000000455
Crash State:
  Exiv2::MemIo::read
  Exiv2::BasicIo::readOrThrow
  Exiv2::QuickTimeVideo::tagDecoder

Sanitizer: address (ASAN)

Recommended Security Severity: High

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

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5744443654799360

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 Wed, Sep 7, 2022, 3:05 PM EDT Project Member

Labels: Disclosure-2022-12-01

Comment 2 by ClusterFuzz-External on Thu, Sep 22, 2022, 1:06 PM EDT Project Member

Status: Verified (was: New)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5744443654799360 is verified as fixed in https://oss-fuzz.com/revisions?job=honggfuzz_asan_exiv2&range=202209210607:202209220613

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

Comment 3 by sheriffbot on Thu, Sep 22, 2022, 2:55 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot