Starred by 2 users

Owner:	wtc@google.com
CC:	wtc@google.com joedr...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Sep 10, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-libavif
Reported-2020-08-11

Issue 24811: libavif:avif_decode_fuzzer: Crash in avifDecoderDataFillImageGrid

Reported by ClusterFuzz-External on Tue, Aug 11, 2020, 1:53 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5201315165372416

Project: libavif
Fuzzing Engine: libFuzzer
Fuzz Target: avif_decode_fuzzer
Job Type: libfuzzer_asan_libavif
Platform Id: linux

Crash Type: UNKNOWN WRITE
Crash Address: 0x7fb81ac821a0
Crash State:
  avifDecoderDataFillImageGrid
  avifDecoderNextImage
  avif_decode_fuzzer.cc

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_libavif&range=202006290220:202006300220

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5201315165372416

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 ClusterFuzz-External on Tue, Aug 11, 2020, 10:09 AM EDT Project Member

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

ClusterFuzz testcase 5201315165372416 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_libavif&range=202008100624:202008110612

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

Comment 2 by wtc@google.com on Tue, Aug 11, 2020, 1:32 PM EDT Project Member

Owner: wtc@google.com

This bug is a duplicate of ~~bug-oss-fuzz:24728~~ and ~~bug-oss-fuzz:24734~~. It is also fixed by the following two commits:
https://github.com/AOMediaCodec/libavif/commit/0a8e7244d494ae98e9756355dfbfb6697ded2ff9
https://github.com/AOMediaCodec/libavif/commit/2fb636141296abdf608f381aa006ddad21a9507a

Comment 3 by sheriffbot on Thu, Sep 10, 2020, 4:05 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot