Starred by 2 users

Owner: ----

CC: kemp...@gmail.com
tfoucu@google.com
micha...@gmx.at
ffmpe...@ffmpeg.org
mich...@niedermayer.cc
jrummell@google.com
twsmith@mozilla.com

Status: Verified *(Closed)*

Components: ----

Modified: Mar 30, 2020

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Proj-ffmpeg
Engine-libfuzzer
OS-Linux
Security_Severity-High
Reported-2019-12-29
Disclosure-2020-03-30

Issue 19734: ffmpeg:ffmpeg_BSF_TRACE_HEADERS_fuzzer: Heap-buffer-overflow in cbs_jpeg_split_fragment

Reported by ClusterFuzz-External on Sun, Dec 29, 2019, 10:49 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5673285471961088

Project: ffmpeg
Fuzzing Engine: libFuzzer
Fuzz Target: ffmpeg_BSF_TRACE_HEADERS_fuzzer
Job Type: libfuzzer_asan_ffmpeg
Platform Id: linux

Crash Type: Heap-buffer-overflow WRITE {*}
Crash Address: 0x60e0000004c2
Crash State:
  cbs_jpeg_split_fragment
  ff_cbs_read_packet
  trace_headers

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_ffmpeg&range=201912060352:201912090352

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5673285471961088

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@chromium.org on Sun, Dec 29, 2019, 11:47 AM EST Project Member

Labels: Disclosure-2020-03-30

Comment 2 by ClusterFuzz-External on Mon, Mar 9, 2020, 1:07 PM EDT Project Member

Cc: twsmith@mozilla.com

Comment 3 by ClusterFuzz-External on Thu, Mar 12, 2020, 10:34 AM EDT Project Member

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

ClusterFuzz testcase 5673285471961088 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_ffmpeg&range=202003100213:202003120213

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

Comment 4 by sheriffbot on Mon, Mar 30, 2020, 2:58 PM EDT Project Member

Labels: -restrict-view-commit

This bug has exceeded our disclosure deadline. It has been opened to the public.

- Your friendly Sheriffbot