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:	Dec 5, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Proj-ffmpeg
OS-Linux
Engine-afl
Security_Severity-High
Reported-2020-10-24
Disclosure-2021-01-22

Issue 26622: ffmpeg:ffmpeg_dem_VIVIDAS_fuzzer: Heap-buffer-overflow in avio_read

Reported by ClusterFuzz-External on Sat, Oct 24, 2020, 1:45 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=6581200338288640

Project: ffmpeg
Fuzzing Engine: afl
Fuzz Target: ffmpeg_dem_VIVIDAS_fuzzer
Job Type: afl_asan_ffmpeg
Platform Id: linux

Crash Type: Heap-buffer-overflow WRITE {*}
Crash Address: 0x6150000001e5
Crash State:
  avio_read
  track_header
  viv_read_header

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_ffmpeg&range=202010140609:202010150617

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=6581200338288640

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 Sat, Oct 24, 2020, 3:00 PM EDT Project Member

Labels: Disclosure-2021-01-22

Comment 2 by ClusterFuzz-External on Thu, Nov 5, 2020, 10:59 AM EST Project Member

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

ClusterFuzz testcase 6581200338288640 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_ffmpeg&range=202011040624:202011050607

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

Comment 3 by sheriffbot on Sat, Dec 5, 2020, 2:53 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