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: Jan 4, 2021

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Proj-ffmpeg
OS-Linux
Engine-afl
Security_Severity-High
Disclosure-2021-01-18
Reported-2020-10-20

Issue 26532: ffmpeg:ffmpeg_AV_CODEC_ID_EXR_fuzzer: Heap-buffer-overflow in decode_frame

Reported by ClusterFuzz-External on Tue, Oct 20, 2020, 11:08 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5613925708857344

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

Crash Type: Heap-buffer-overflow WRITE {*}
Crash Address: 0x6170000002cf
Crash State:
  decode_frame
  decode_simple_internal
  decode_simple_receive_frame

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_ffmpeg&range=202009110608:202009120617

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5613925708857344

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 Tue, Oct 20, 2020, 3:03 PM EDT Project Member

Labels: Disclosure-2021-01-18

Comment 2 by ClusterFuzz-External on Mon, Nov 23, 2020, 10:23 AM EST Project Member

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

ClusterFuzz testcase 5613925708857344 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_ffmpeg&range=202011220603:202011230602

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

Comment 3 by sheriffbot on Wed, Dec 23, 2020, 2:52 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

Comment 4 by aberg...@gmail.com on Mon, Jan 4, 2021, 8:43 AM EST

CVE-2020-35965 was assigned to this issue.

Reference:
https://nvd.nist.gov/vuln/detail/CVE-2020-35965