☆ Starred by 1 user

Owner:	----
CC:	boxe...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Apr 23, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-grok
Reported-2021-04-22
Disclosure-2021-07-21

Issue 33544: grok:grk_decompress_fuzzer: Heap-buffer-overflow in grk::FileFormatDecompress::apply_palette_clr

Reported by ClusterFuzz-External on Wed, Apr 21, 2021, 10:15 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5022555195965440

Project: grok
Fuzzing Engine: libFuzzer
Fuzz Target: grk_decompress_fuzzer
Job Type: libfuzzer_asan_grok
Platform Id: linux

Crash Type: Heap-buffer-overflow WRITE 16
Crash Address: 0x7fac177cd800
Crash State:
  grk::FileFormatDecompress::apply_palette_clr
  grk::FileFormatDecompress::applyColour
  grk_decompress_fuzzer.cpp

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_grok&range=202101210604:202101220605

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5022555195965440

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 Thu, Apr 22, 2021, 3:02 PM EDT Project Member

Labels: Disclosure-2021-07-21

Comment 2 by boxe...@gmail.com on Thu, Apr 22, 2021, 7:58 PM EDT Project Member

Status: Fixed (was: New)

Fixed by 1d9086205a0e91fb6517ebb09b00af354431f468

Comment 3 by ClusterFuzz-External on Fri, Apr 23, 2021, 10:33 AM EDT Project Member

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

ClusterFuzz testcase 5022555195965440 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_grok&range=202104220620:202104230622

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

Comment 4 by sheriffbot on Fri, Apr 23, 2021, 2:51 PM EDT Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot