Starred by 2 users

Owner:	----
CC:	a...@adalogics.com taking@google.com kusano@google.com dbloomberg@google.com stjow...@googlemail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Jun 10, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Engine-afl
Security_Severity-Medium
Proj-leptonica
Reported-2020-05-10

Issue 22140: leptonica:colorquant_fuzzer: Heap-buffer-overflow in pixFewColorsOctcubeQuantMixed

Reported by ClusterFuzz-External on Sun, May 10, 2020, 5:20 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5688942482685952

Project: leptonica
Fuzzing Engine: afl
Fuzz Target: colorquant_fuzzer
Job Type: afl_asan_leptonica
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 1
Crash Address: 0x6020000003bf
Crash State:
  pixFewColorsOctcubeQuantMixed
  colorquant_fuzzer.cc

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_leptonica&range=202005062344:202005070249

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5688942482685952

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 dbloomberg@google.com on Mon, May 11, 2020, 2:28 PM EDT Project Member

Status: Fixed (was: New)

Should now be fixed.

Comment 2 by ClusterFuzz-External on Tue, May 12, 2020, 11:31 AM EDT Project Member

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

ClusterFuzz testcase 5688942482685952 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_leptonica&range=202005110214:202005120215

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

Comment 3 by sheriffbot on Wed, Jun 10, 2020, 4:07 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