☆ Starred by 1 user

Owner:	----
CC:	a...@adalogics.com taking@google.com kusano@google.com dbloomberg@google.com stjow...@googlemail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Jun 3, 2020
Type:	Bug

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Stability-UndefinedBehaviorSanitizer
Engine-libfuzzer
OS-Linux
Proj-leptonica
Reported-2020-05-03
Disclosure-2020-08-03

Issue 21997: leptonica:barcode_fuzzer: Undefined-shift in pixConvert2To8

Reported by ClusterFuzz-External on Sun, May 3, 2020, 7:42 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5719749863669760

Project: leptonica
Fuzzing Engine: libFuzzer
Fuzz Target: barcode_fuzzer
Job Type: libfuzzer_ubsan_leptonica
Platform Id: linux

Crash Type: Undefined-shift
Crash Address:
Crash State:
  pixConvert2To8
  pixProcessBarcodes
  barcode_fuzzer.cc

Sanitizer: undefined (UBSAN)

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_leptonica&range=202005020213:202005030215

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5719749863669760

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 stjow...@googlemail.com on Sun, May 3, 2020, 1:29 PM EDT

Pull request https://github.com/DanBloomberg/leptonica/pull/499 now includes a commit which fixes this issue.

Comment 2 by sheriffbot on Sun, May 3, 2020, 4:11 PM EDT Project Member

Labels: Disclosure-2020-08-03

Comment 3 by ClusterFuzz-External on Mon, May 4, 2020, 1:19 PM EDT Project Member

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

ClusterFuzz testcase 5719749863669760 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_leptonica&range=202005030215:202005040614

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

Comment 4 by sheriffbot on Wed, Jun 3, 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

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy