




☆ 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:** Jul 15, 2020

**Type:** [Bug-Security](#)

[ClusterFuzz](#)  
[Stability-Memory-AddressSanitizer](#)  
[Reproducible](#)  
[ClusterFuzz-Verified](#)  
[OS-Linux](#)  
[Security\\_Severity-Medium](#)  
[Proj-leptonica](#)  
[Engine-honggfuzz](#)  
[Reported-2020-06-14](#)  
[Disclosure-2020-09-14](#)

## Issue 23433: leptonica:ccbord\_fuzzer: Heap-buffer-overflow in findNextBorderPixel

Reported by [ClusterFuzz-External](#) on Sun, Jun 14, 2020, 5:08 AM EDT [Project Member](#)

 [Code](#)

Detailed Report: <https://oss-fuzz.com/testcase?key=5068431018950656>

Project: leptonica  
Fuzzing Engine: honggfuzz  
Fuzz Target: ccbord\_fuzzer  
Job Type: honggfuzz\_asan\_leptonica  
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 4  
Crash Address: 0x612000000924  
Crash State:  
findNextBorderPixel  
pixGetHoleBorder  
pixGetCCBorders

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: [https://oss-fuzz.com/revisions?job=honggfuzz\\_asan\\_leptonica&range=202005070249:202005080213](https://oss-fuzz.com/revisions?job=honggfuzz_asan_leptonica&range=202005070249:202005080213)

Reproducer Testcase: [https://oss-fuzz.com/download?testcase\\_id=5068431018950656](https://oss-fuzz.com/download?testcase_id=5068431018950656)

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 Sun, Jun 14, 2020, 4:08 PM EDT [Project Member](#)

**Labels:** [Disclosure-2020-09-14](#)

Comment 2 by [dbloomberg@google.com](mailto:dbloomberg@google.com) on Mon, Jun 15, 2020, 1:54 AM EDT Project Member

**Status:** Fixed (was: New)

believe it is fixed: Check pix boundary when looking for the next pixel.

Comment 3 by [ClusterFuzz-External](#) on Tue, Jun 16, 2020, 10:25 AM EDT Project Member

**Status:** Verified (was: Fixed)

**Labels:** ClusterFuzz-Verified

ClusterFuzz testcase 5068431018950656 is verified as fixed in [https://oss-fuzz.com/revisions?job=honggfuzz\\_asan\\_leptonica&range=202006150223:202006160222](https://oss-fuzz.com/revisions?job=honggfuzz_asan_leptonica&range=202006150223:202006160222)

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

Comment 4 by [sheriffbot](#) on Wed, Jul 15, 2020, 3:59 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