Starred by 2 users

Owner:	----
CC:	a...@adalogics.com taking@google.com kusano@google.com dbloomberg@google.com stjow...@googlemail.com
Status:	Fixed *(Closed)*
Components:	----
Modified:	Jun 26, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
Engine-libfuzzer
OS-Linux
Needs-Feedback
Security_Severity-Medium
Proj-leptonica
Disclosure-2020-08-24
Reported-2020-05-26

Issue 22512: leptonica:pageseg_fuzzer: Heap-buffer-overflow in rasteropGeneralLow

Reported by ClusterFuzz-External on Tue, May 26, 2020, 6:58 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5744295188627456

Project: leptonica
Fuzzing Engine: libFuzzer
Fuzz Target: pageseg_fuzzer
Job Type: libfuzzer_asan_leptonica
Platform Id: linux

Crash Type: Heap-buffer-overflow READ 4
Crash Address: 0x602000000498
Crash State:
  rasteropGeneralLow
  rasteropLow
  pixRasterop

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_leptonica&range=202005130216:202005140617

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5744295188627456

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, May 26, 2020, 4:13 PM EDT Project Member

Labels: Disclosure-2020-08-24

Comment 2 by dbloomberg@google.com on Wed, May 27, 2020, 1:48 PM EDT Project Member

Status: Fixed (was: New)

This is a strange error. The rasterop part of the library has been fairly extensively tested.
Simplifying the hole filling function where this happens. Hope it fixes the issue.

Comment 3 by ClusterFuzz-External on Wed, Jun 3, 2020, 2:08 PM EDT Project Member

Labels: Needs-Feedback

ClusterFuzz testcase 5744295188627456 is still reproducing on tip-of-tree build (trunk).

Please re-test your fix against this testcase and if the fix was incorrect or incomplete, please re-open the bug. Otherwise, ignore this notification and add the ClusterFuzz-Wrong label.

Comment 4 by dbloomberg@google.com on Thu, Jun 11, 2020, 1:50 AM EDT Project Member

~~Issue 22280~~ has been merged into this issue.

Comment 5 by sheriffbot on Fri, Jun 26, 2020, 4:02 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