Starred by 2 users

Owner:	----
CC:	sebas...@artifex.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Feb 27, 2020
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-jbig2dec
Reported-2020-01-25
Disclosure-2020-04-24

Issue 20332: jbig2dec:jbig2_fuzzer: Heap-buffer-overflow in template_image_compose_opt

Reported by ClusterFuzz-External on Sat, Jan 25, 2020, 4:58 PM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5647271708590080

Project: jbig2dec
Fuzzing Engine: libFuzzer
Fuzz Target: jbig2_fuzzer
Job Type: libfuzzer_asan_jbig2dec
Platform Id: linux

Crash Type: Heap-buffer-overflow WRITE 1
Crash Address: 0x7f67ba2dec7c
Crash State:
  template_image_compose_opt
  jbig2_image_compose_opt_REPLACE
  jbig2_image_compose

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_jbig2dec&range=202001230422:202001240425

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5647271708590080

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@chromium.org on Sun, Jan 26, 2020, 1:29 PM EST Project Member

Labels: Disclosure-2020-04-24

Comment 2 by ClusterFuzz-External on Tue, Jan 28, 2020, 10:27 AM EST Project Member

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

ClusterFuzz testcase 5647271708590080 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_jbig2dec&range=202001270433:202001280430

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

Comment 3 by sheriffbot on Thu, Feb 27, 2020, 3:02 PM EST Project Member

Labels: -restrict-view-commit

This bug has been fixed for 30 days. It has been opened to the public.

- Your friendly Sheriffbot