Starred by 2 users

Owner: ----

CC: paul....@gmail.com
alex....@gmail.com
bobjf...@gmail.com
tro...@gmail.com

Status: Verified *(Closed)*

Components: ----

Modified: May 31, 2020

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Deadline-Exceeded
Stability-AFL
OS-Linux
Engine-afl
Proj-graphicsmagick
Security_Severity-High
Reported-2019-11-20
Disclosure-2020-02-18

Issue 19025: graphicsmagick:coder_MNG_fuzzer: Heap-buffer-overflow in ReadMNGImage

Reported by ClusterFuzz-External on Wed, Nov 20, 2019, 11:06 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=6322015271387136

Project: graphicsmagick
Fuzzing Engine: afl
Fuzz Target: coder_MNG_fuzzer
Job Type: afl_asan_graphicsmagick
Platform Id: linux

Crash Type: Heap-buffer-overflow WRITE 8
Crash Address: 0x6150000261d7
Crash State:
  ReadMNGImage
  ReadImage
  BlobToImage

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_graphicsmagick&range=201807100603:201807102347

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=6322015271387136

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 Wed, Nov 20, 2019, 11:52 AM EST Project Member

Labels: Disclosure-2020-02-18

Comment 2 by sheriffbot on Tue, Feb 11, 2020, 1:01 PM EST Project Member

Labels: Deadline-Approaching

This bug is approaching its deadline for being fixed, and will be automatically derestricted within 7 days. If a fix is planned within 2 weeks after the deadline has passed, a grace extension can be granted.

- Your friendly Sheriffbot

Comment 3 by sheriffbot on Tue, Feb 18, 2020, 1:16 PM EST Project Member

Labels: -restrict-view-commit -deadline-approaching Deadline-Exceeded

This bug has exceeded our disclosure deadline. It has been opened to the public.

- Your friendly Sheriffbot

Comment 4 by bobjf...@gmail.com on Sun, May 31, 2020, 9:46 AM EDT

Fixed by Mercurial changeset 16291:50395430a371.

Comment 5 by ClusterFuzz-External on Sun, May 31, 2020, 10:38 AM EDT Project Member

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

ClusterFuzz testcase 6322015271387136 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_graphicsmagick&range=202005300143:202005310142

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