☆ Starred by 1 user

Owner:	----
CC:	tsdg...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	May 2, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
OS-Linux
Engine-afl
Security_Severity-High
Proj-kimageformats
Disclosure-2021-07-26
Reported-2021-04-27

Issue 33742: kimageformats:kimgio_xcf_fuzzer: Stack-buffer-overflow in XCFImageFormat::loadTileRLE

Reported by ClusterFuzz-External on Tue, Apr 27, 2021, 7:44 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5535712133906432

Project: kimageformats
Fuzzing Engine: afl
Fuzz Target: kimgio_xcf_fuzzer
Job Type: afl_asan_kimageformats
Platform Id: linux

```
Crash Type: Stack-buffer-overflow WRITE 1
Crash Address: 0x7f8068253938
Crash State:
  XCFImageFormat::loadTileRLE
  XCFImageFormat::loadLevel
  XCFImageFormat::loadHierarchy
```

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_kimageformats&range=202004130222:202004170222

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5535712133906432

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, Apr 27, 2021, 3:09 PM EDT Project Member

Labels: Disclosure-2021-07-26

Comment 2 by ClusterFuzz-External on Sun, May 2, 2021, 11:02 AM EDT Project Member

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

ClusterFuzz testcase 5535712133906432 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_kimageformats&range=202105010606:202105020632

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

Comment 3 by sheriffbot on Sun, May 2, 2021, 2:56 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed. It has been opened to the public.

- Your friendly Sheriffbot