oss-fuzz oss-fuzz ▾ New issue Open issues ▾ Search oss-fuzz issues... ▾ Sign in

☆ Starred by 1 user

Owner:	----
CC:	atho...@thinkspatial.com.au juerg...@gmail.com bisho...@gmail.com mate...@loskot.net schw...@gmail.com nyall...@gmail.com even....@gmail.com ari.j...@gmail.com bjorn...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	15 days ago
Type:	Bug

ClusterFuzz
Reproducible
ClusterFuzz-Verified
Stability-UndefinedBehaviorSanitizer
Engine-libfuzzer
OS-Linux
Proj-gdal
Disclosure-2023-02-06
Reported-2022-11-08

Issue 53137: gdal:dimap_fuzzer: Unsigned-integer-overflow in gdal_TIFFReadRGBATileExt

Reported by ClusterFuzz-External on Tue, Nov 8, 2022, 8:40 AM EST (17 days ago) Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5738253143900160

Project: gdal
Fuzzing Engine: libFuzzer
Fuzz Target: dimap_fuzzer
Job Type: libfuzzer_ubsan_gdal
Platform Id: linux

Crash Type: Unsigned-integer-overflow
Crash Address:
Crash State:
  gdal_TIFFReadRGBATileExt
  GTiffRGBABand::IReadBlock
  GDALRasterBand::GetLockedBlockRef

Sanitizer: undefined (UBSAN)

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_gdal&range=202109180604:202109190613

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5738253143900160

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 even....@gmail.com on Tue, Nov 8, 2022, 9:17 AM EST (17 days ago)

fix in libtiff in https://gitlab.com/libtiff/libtiff/-/merge_requests/410

Comment 2 by sheriffbot on Tue, Nov 8, 2022, 2:57 PM EST (17 days ago) Project Member

Labels: Disclosure-2023-02-06

Comment 3 by ClusterFuzz-External on Thu, Nov 10, 2022, 10:36 AM EST (15 days ago) Project Member

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

ClusterFuzz testcase 5738253143900160 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_ubsan_gdal&range=202211090602:202211100616

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

Comment 4 by sheriffbot on Thu, Nov 10, 2022, 2:46 PM EST (15 days ago) Project Member

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy