☆ Starred by 2 users

Owner:	----
CC:	stjow...@googlemail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Mar 8, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-tesseract-ocr
Disclosure-2021-04-19
Reported-2021-01-18

Issue 29698: tesseract-ocr:fuzzer-api-512x256: Heap-use-after-free in __libcpp_strpbrk

Reported by ClusterFuzz-External on Mon, Jan 18, 2021, 4:11 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=4656898932604928

Project: tesseract-ocr
Fuzzing Engine: libFuzzer
Fuzz Target: fuzzer-api-512x256
Job Type: libfuzzer_asan_tesseract-ocr
Platform Id: linux

Crash Type: Heap-use-after-free READ 2
Crash Address: 0x60400027d390
Crash State:
  __libcpp_strpbrk
  strpbrk
  tesseract::Tesseract::one_ell_conflict

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_tesseract-ocr&range=202012250604:202012300619

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=4656898932604928

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 Mon, Jan 18, 2021, 3:03 PM EST Project Member

Labels: Disclosure-2021-04-19

Comment 2 by ClusterFuzz-External on Sat, Feb 6, 2021, 11:08 AM EST Project Member

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

ClusterFuzz testcase 4656898932604928 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_tesseract-ocr&range=202102050613:202102060619

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

Comment 3 by sheriffbot on Mon, Mar 8, 2021, 2:52 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