Starred by 2 users

Owner: ----

CC: l...@wolfssl.com
kaleb...@gmail.com
da...@wolfssl.com
ja...@wolfssl.com
guido...@gmail.com
john....@gmail.com
j...@wolfssl.com
ka...@wolfssl.com
test...@wolfssl.com

Status: Verified *(Closed)*

Components: ----

Modified: Dec 5, 2020

Type: Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Proj-wolfssl
Security_Severity-High
Reported-2020-10-21
Disclosure-2021-01-19

Issue 26567: wolfssl:fuzzer-wolfssl-rsa: Heap-buffer-overflow in RsaPad_PSS

Reported by ClusterFuzz-External on Wed, Oct 21, 2020, 5:03 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5717341540974592

Project: wolfssl
Fuzzing Engine: libFuzzer
Fuzz Target: fuzzer-wolfssl-rsa
Job Type: libfuzzer_asan_wolfssl
Platform Id: linux

Crash Type: Heap-buffer-overflow WRITE {*}
Crash Address: 0x60d000000337
Crash State:
  RsaPad_PSS
  wc_RsaPad_ex
  RsaPublicEncryptEx

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_wolfssl&range=202009220626:202009230602

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5717341540974592

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 Thu, Oct 22, 2020, 3:03 PM EDT Project Member

Labels: Disclosure-2021-01-19

Comment 2 by ClusterFuzz-External on Wed, Nov 4, 2020, 10:34 AM EST Project Member

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

ClusterFuzz testcase 5717341540974592 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_wolfssl&range=202011030610:202011040605

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

Comment 3 by sheriffbot on Sat, Dec 5, 2020, 2:53 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