▼ Q Search oss-fuzz issues... oss-fuzz oss-fuzz ▼ New issue Open issues ☆ Starred by 1 user Owner: CC: omosn...@gmail.com evv...@gmail.com jwca...@gmail.com nicol...@m4x.org nicol...@gmail.com Status: Verified (Closed) Apr 21, 2021 Modified: Bug-Security Type: ClusterFuzz Stability-Memory-AddressSanitizer Reproducible ClusterFuzz-Verified Engine-libfuzzer OS-Linux Security_Severity-High Proj-selinux Reported-2021-02-18 Disclosure-2021-05-19

Sign in

Issue 31065: selinux:secilc-fuzzer: Heap-use-after-free in __cil_verify_classperms

Reported by ClusterFuzz-External on Wed, Feb 17, 2021, 9:08 PM EST

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5453822921146368

Project: selinux Fuzzing Engine: libFuzzer Fuzz Target: secilc-fuzzer
Job Type: libfuzzer_asan_selinux Platform Id: linux

Crash Type: Heap-use-after-free READ 8 Crash Address: 0x603000014cb8 Crash State: __cil_verify_classperms __cil_verify_classpermission

__cil_pre_verify_helper Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_selinux&range=202102171200:202102171800

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5453822921146368

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://gilthub.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 Fri, Feb 19, 2021, 3:04 PM EST Project Member

Labels: Disclosure-2021-05-19

Comment 2 by ClusterFuzz-External on Tue, Apr 20, 2021, 10:32 AM EDT Project Member

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

ClusterFuzz testcase 5453822921146368 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_selinux&range=202104191800:202104200000

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

Comment 3 by sheriffbot on Wed, Apr 21, 2021, 2:52 PM EDT Project Member

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