

☆ Starred by 1 user

Owner: ----

CC: [omoshn...@gmail.com](#)
[evv...@gmail.com](#)
[jwca...@gmail.com](#)
[nicol...@m4x.org](#)
[nicol...@gmail.com](#)

Status: Verified (Closed)

Components: ----

Modified: Apr 21, 2021

Type: [Bug-Security](#)

[ClusterFuzz](#)
[Stability-Memory-AddressSanitizer](#)
[Reproducible](#)
[ClusterFuzz-Verified](#)
[Engine-libfuzzer](#)
[OS-Linux](#)
[Security_Severity-High](#)
[Proj-selinux](#)
[Reported-2021-03-18](#)
[Disclosure-2021-06-16](#)

Issue 32177: selinux:secilc-fuzzer: Heap-use-after-free in cil_reset_classpermission

Reported by [ClusterFuzz-External](#) on Thu, Mar 18, 2021, 7:16 AM EDT Project Member

 Code

Detailed Report: <https://oss-fuzz.com/testcase?key=6087260287139840>

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: 0x60400000130
Crash State:
cil_reset_classpermission
cil_reset_classperms_set
cil_reset_classperms_list

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=6087260287139840

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, Mar 18, 2021, 3:08 PM EDT Project Member

Labels: [Disclosure-2021-06-16](#)

[Comment 2](#) by [ClusterFuzz-External](#) on Tue, Apr 20, 2021, 11:28 AM EDT Project Member

Status: Verified (was: New)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 6087260287139840 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

Labels: -restrict-view-commit

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

- Your friendly Sheriffbot