Starred by 1 user

Owner:	----
CC:	omosn...@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-Medium
Proj-selinux
Disclosure-2021-06-28
Reported-2021-03-30

Issue 32675: selinux:secilc-fuzzer: Heap-buffer-overflow in ebitmap_match_any

Reported by ClusterFuzz-External on Tue, Mar 30, 2021, 5:05 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5563841674084352

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

Crash Type: Heap-buffer-overflow READ 8
Crash Address: 0x7f7e49d387f0
Crash State:
  ebitmap_match_any
  avtab_map
  cil_check_neverallow

Sanitizer: address (ASAN)

Recommended Security Severity: Medium

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

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5563841674084352

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 Wed, Mar 31, 2021, 3:02 PM EDT Project Member

Labels: Disclosure-2021-06-28

Comment 2 by ClusterFuzz-External on Tue, Apr 20, 2021, 10:35 AM EDT Project Member

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

ClusterFuzz testcase 5563841674084352 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