☆ Starred by 2 users

Owner:	----
CC:	sta...@stalkr.net keyst...@gmail.com p.ant...@catenacyber.fr
Status:	Verified *(Closed)*
Components:	----
Modified:	Feb 6, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Deadline-Exceeded
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-keystone
Reported-2020-05-20
Disclosure-2020-08-18

Issue 22371: keystone:fuzz_asm_sparc64be: Invalid-free in llvm_ks::SmallVectorImpl<llvm_ks::MCFixup>::~SmallVectorImpl

Reported by ClusterFuzz-External on Wed, May 20, 2020, 3:12 AM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5767140656545792

Project: keystone
Fuzzing Engine: libFuzzer
Fuzz Target: fuzz_asm_sparc64be
Job Type: libfuzzer_asan_keystone
Platform Id: linux

Crash Type: Invalid-free
Crash Address: 0x61900000059d
Crash State:
  llvm_ks::SmallVectorImpl<llvm_ks::MCFixup>::~SmallVectorImpl
  llvm_ks::MCEncodedFragmentWithFixups<32u, 4u>::~MCEncodedFragmentWithFixups
  llvm_ks::MCFragment::destroy

Sanitizer: address (ASAN)

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_keystone&range=202005130212:202005140614

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5767140656545792

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, May 20, 2020, 4:19 PM EDT Project Member

Labels: Disclosure-2020-08-18

Comment 2 by sheriffbot on Tue, Aug 11, 2020, 3:57 PM EDT Project Member

Labels: Deadline-Approaching

This bug is approaching its deadline for being fixed, and will be automatically derestricted within 7 days. If a fix is planned within 2 weeks after the deadline has passed, a grace extension can be granted.

- Your friendly Sheriffbot

Comment 3 by sheriffbot on Tue, Aug 18, 2020, 4:02 PM EDT Project Member

Labels: -restrict-view-commit -deadline-approaching Deadline-Exceeded

This bug has exceeded our disclosure deadline. It has been opened to the public.

- Your friendly Sheriffbot

Comment 4 by ClusterFuzz-External on Mon, Nov 9, 2020, 11:47 AM EST Project Member

Cc: sta...@stalkr.net

Comment 5 by ClusterFuzz-External on Sat, Feb 6, 2021, 10:36 AM EST Project Member

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

ClusterFuzz testcase 5767140656545792 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_keystone&range=202102050606:202102060600

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