☆ 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
OS-Linux
Engine-afl
Security_Severity-High
Proj-keystone
Reported-2020-05-30
Disclosure-2020-08-28

Issue 22850: keystone:fuzz_asm_x86_16: Heap-use-after-free in llvm_ks::X86Operand::getToken

Reported by ClusterFuzz-External on Sat, May 30, 2020, 3:43 PM EDT Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5637154293415936

Project: keystone
Fuzzing Engine: afl
Fuzz Target: fuzz_asm_x86_16
Job Type: afl_asan_keystone
Platform Id: linux

Crash Type: Heap-use-after-free READ 4
Crash Address: 0x60d000000a28
Crash State:
  llvm_ks::X86Operand::getToken
  X86AsmParser::MatchAndEmitATTInstruction
  X86AsmParser::MatchAndEmitInstruction

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=afl_asan_keystone&range=201911200413:201911222344

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5637154293415936

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 Sat, May 30, 2020, 4:12 PM EDT Project Member

Labels: Disclosure-2020-08-28

Comment 2 by sheriffbot on Fri, Aug 21, 2020, 3:58 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 Fri, Aug 28, 2020, 4:01 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, 11:49 AM EST Project Member

Cc: sta...@stalkr.net

Comment 5 by ClusterFuzz-External on Sat, Feb 6, 2021, 11:26 AM EST Project Member

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

ClusterFuzz testcase 5637154293415936 is verified as fixed in https://oss-fuzz.com/revisions?job=afl_asan_keystone&range=202102050606:202102060600

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