Contribution ID: **161** Type: **not specified**

Lightning Talk: Fuzzing glibc's iconv program

Tuesday, August 25, 2020 8:30 AM (10 minutes)

A while back, I found myself triaging an iconv bug report that found hangs in the program when run with certain inputs. Not knowing a lot about iconv internals, I wrote a rudimentary fuzzer to investigate the problem, which caught over 160 different input combinations that led to hangs and a clear pattern hinting at the cause.

In this short talk, I'll share my experiences with fuzzing iconv and eventually cleaning up some of the iconv front-end with a patch.

I agree to abide by the anti-harassment policy

I agree

Primary author: SHANKAR, Arjun (Red Hat)

Presenter: SHANKAR, Arjun (Red Hat)

Session Classification: GNU Tools Track

Track Classification: GNU Tools Track