tetanus-shot

by willsroot / Albytross

Tags: cve pwn heap rust cve-2018-1000657

Rating: 5.0

Program compiled with Rustc 1.19 nightly (as discovered by strings), which is vulnerable in the VecDeque::reserve() function (CVE-2018-1000657). Can be leveraged to have an 8 byte overflow into the size metadata of the next chunk in this program. By utilizing the 8 byte overflow to expand chunk sizes, chunks that come afterwards in memory can be overlapped, allowing for classic heap attacks (the glibc allocator is used).

Original writeup (https://www.willsroot.io/2020/06/redpwnctf-2020-rust-pwn-writeups.html).

Comments