tetanus

by willsroot / Albytross

Tags: pwn heap rust

Rating: 5.0

Rust program uses the glibc allocator and uses unsafe code when deleting from the list. Allows for UAF and double free. Make sure to bypass the double free protection mechanism for tcache on this libc version (2.30) when developing this exploit.

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

Comments

Follow @CTFtime