four-function-heap

by willsroot / Albytross

Tags: heap pwn

Rating:

Classic heap problem with 4 options (add, delete, show, exit) and a UAF vulnerability on libc 2.27. Only 14 moves allowed. Manipulate the tcache chunk counts and the pointers stored on the tcache_perthread_struct in order to leverage the UAF to a shell in 14 moves.

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

Comments