A3

A1

A3

Input 1

Thread A - ioctl(CREATE_VCPU)	
A2	if (atomic_fetch_add(kvm->re

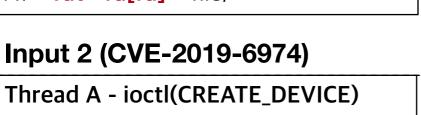
BUG()

fdt->fd[fd] = file;

BUG()

fetch add(kvm->refcnt) == 0)fdt->fd[fd] = file;

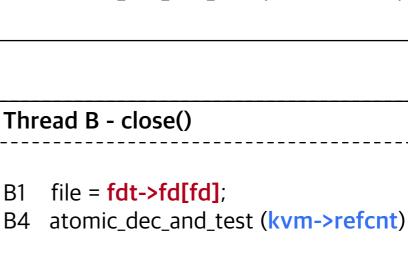






Thread B - close()

file = fdt->fd[fd];



atomic dec and test (kvm->refcnt)