Input 1

Thread A - open(O_CREAT)	Thread B - close()
/* In fd_install() */ A1 fdt->fd[fd] = file;	/* In close_fd() */ B1 file = fdt->fd[fd];

Input 2

Thread A - ioctl(CREATE_VCPU)	Thread B - close()
/* In kvm_get_kvm() */ A2 if ((kvm->refcnt++) == 0) A3 BUG()	/* In kvm_put_kvm() */ B4 if ((--kvm->refcnt) == 0) B5 destory_vm(kvm);

Input 3 (CVE-2019-6974)

Thread A - ioctl(CREATE_DEVICE)	Thread B - close()
A1 fdt->fd[fd] = file; A2 if ((kvm->refcnt++) == 0) A3 BUG()	B1 file = fdt->fd[fd]; B4 if ((--kvm->refcnt) == 0) B5 destory_vm(kvm);