

Input 1

Thread A - ioctl(CREATE_VCPU)

A2 if (atomic_fetch_add(**kvm->refcnt**)
== 0)
A3 BUG()
A1 **fdt->fd[fd]** = file;

Thread B - close()

B1 file = **fdt->fd[fd]**;
B4 atomic_dec_and_test (**kvm->refcnt**)

Input 2 (CVE-2019-6974)

Thread A - ioctl(CREATE_DEVICE)

A1 **fdt->fd[fd]** = file;
A2 if (atomic_fetch_add(**kvm->refcnt**)
== 0)
A3 BUG()

Thread B - close()

B1 file = **fdt->fd[fd]**;
B4 atomic_dec_and_test (**kvm->refcnt**)