

Thread A - mmap()

```
/* In binder_mmap() */  
A1  alloc->vma = vma;  
  
A2  alloc->mm = vma->mm;
```

Thread B - ioctl(TRANSACTION)

```
/* In binder_alloc_new_buf() */  
B1  vma = alloc->vma  
B2  if (alloc->vma == NULL)  
B3      return;  
/* In binder_update_page() */  
B4  atomic_inc(&alloc->mm->refcount);
```