

// Thread msync

```
static int msync_interval(...) {  
...  
    struct file * file = vma->vm_file;  
...  
    if(file->f_op&&file->f_op->fsync){  
        err = file->f_op->fsync(...);  
    }  
}
```

vulnerable site



// Thread uselib

```
int do_munmap(...) {  
...  
    file->f_op = NULL;  
...  
}
```

file->f\_op = NULL;

...

}

err = file->f\_op->fsync(...);

file->f\_op = NULL;

...

}