



author Dmitry Osipenko <dmitry.osipenko@collabora.com> 2023-01-09 00:13:11 +0300
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-22 13:31:34 +0100
commit 5cfb617967b05f8f27e862c97db1fabd8485f4db (patch)
tree 03711c9aaffa734d44f9616d15c8a3c32fc36743
parent d1d826954475db4e7cff9fe614f2be4c94c35d5a (diff)
download linux-5cfb617967b05f8f27e862c97db1fabd8485f4db.tar.gz

diff options

context: 3
space: include
mode: unified

drm/shmem-helper: Remove another errant put in error path

commit ee9adb7a45516cfa536ca92253d7ae59d56db9e4 upstream.

drm_gem_shmem_mmap() doesn't own reference in error code path, resulting in the dma-buf shmem GEM object getting prematurely freed leading to a later use-after-free.

Fixes: f49a51bfdc8e ("drm/shme-helpers: Fix dma_buf_mmap forwarding bug")

Cc: stable@vger.kernel.org

Signed-off-by: Dmitry Osipenko <dmitry.osipenko@collabora.com>

Reviewed-by: Rob Clark <robdclark@gmail.com>

Link: <https://patchwork.freedesktop.org/patch/msgid/20230108211311.3950107-1-dmitry.osipenko@collabora.com>

Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat

```
-rw-r--r-- drivers/gpu/drm/drm_gem_shmem_helper.c 9
```

1 files changed, 6 insertions, 3 deletions

diff --git a/drivers/gpu/drm/drm_gem_shmem_helper.c b/drivers/gpu/drm/drm_gem_shmem_helper.c

index d58e8e12d3ae8e..0c2968052b663a 100644

--- a/drivers/gpu/drm/drm_gem_shmem_helper.c

+++ b/drivers/gpu/drm/drm_gem_shmem_helper.c

```
@@ -591,11 +591,14 @@ int drm_gem_shmem_mmap(struct drm_gem_shmem_object *shmem, struct vm_area_struct  
    int ret;
```

```
    if (obj->import_attach) {
```

```
-        /* Drop the reference drm_gem_mmap_obj() acquired.*/
```

```
-        drm_gem_object_put(obj);
```

```
    vma->vm_private_data = NULL;
```

```
+        ret = dma_buf_mmap(obj->dma_buf, vma, 0);
```

```
+        ret = dma_buf_mmap(obj->dma_buf, vma, 0);
```

```
+        /* Drop the reference drm_gem_mmap_obj() acquired.*/
```

```
+        if (!ret)
```

```
+            drm_gem_object_put(obj);
```

```
-        return dma_buf_mmap(obj->dma_buf, vma, 0);
```

```
+        return ret;
```

```
    }
```

```
    ret = drm_gem_shmem_get_pages(shmem);
```