

## [PATCH 2.6.15-rc3] Fix NULL-reference in DRM

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-11/9721.html>

---

**From:** Takashi Iwai ([tiwai@suse.de](mailto:tiwai@suse.de))

**Date:** 11/30/05

Date: Wed, 30 Nov 2005 15:32:59 +0100

To: [linux-kernel@vger.kernel.org](mailto:linux-kernel@vger.kernel.org)

This patch fixes the NULL pointer reference in DRM. SiS driver tries to allocate a big chunk of memory, but the return value is never checked.

Reported in Novell bugzilla #132271:

[https://bugzilla.novell.com/show\\_bug.cgi?id=132271](https://bugzilla.novell.com/show_bug.cgi?id=132271)

From: Egbert Eich <[eich@suse.de](mailto:eich@suse.de)>

Signed-off-by: Takashi Iwai <[tiwai@suse.de](mailto:tiwai@suse.de)>

```
diff --git a/drivers/char/drm/drm_context.c b/drivers/char/drm/drm_context.c
```

```
--- a/drivers/char/drm/drm_context.c
```

```
+++ b/drivers/char/drm/drm_context.c
```

```
@@ -432,7 +432,10 @@ int drm_addctx(struct inode *inode, stru
```

```
    if (ctx.handle != DRM_KERNEL_CONTEXT) {
        if (dev->driver->context_ctor)
- dev->driver->context_ctor(dev, ctx.handle);
+ if (!dev->driver->context_ctor(dev, ctx.handle)) {
+ DRM_DEBUG("Running out of ctxs or memory.\n");
+ return -ENOMEM;
+ }
    }
```

```
    ctx_entry = drm_alloc(sizeof(*ctx_entry), DRM_MEM_CTXLIST);
```

```
-
```

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to [majordomo@vger.kernel.org](mailto:majordomo@vger.kernel.org)

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>