

From: "Jason A. Donenfeld" <Jason@zx2c4.com>  
To: dri-devel@lists.freedesktop.org, linux-api@vger.kernel.org,  
linux-kernel@vger.kernel.org  
Cc: "Jason A. Donenfeld" <Jason@zx2c4.com>,  
"Daniel Vetter" <daniel.vetter@intel.com>,  
"Peter Zijlstra" <peterz@infradead.org>,  
"Ilia Mirkin" <imirkin@alum.mit.edu>,  
"Maarten Lankhorst" <maarten.lankhorst@linux.intel.com>,  
"Nicholas Kazlauskas" <nicholas.kazlauskas@amd.com>,  
"Christian Brauner" <brauner@kernel.org>,  
"Michel Dänzer" <michel@daenzer.net>,  
"Alex Deucher" <alexdeucher@gmail.com>,  
"Adam Jackson" <ajax@redhat.com>,  
"Greg Kroah-Hartman" <gregkh@linuxfoundation.org>,  
"Sean Paul" <sean@poorly.run>, "David Airlie" <airlied@linux.ie>,  
"Rob Clark" <robdclark@gmail.com>,  
"Sultan Alsawaf" <sultan@kerneltoast.com>  
Subject: [PATCH] drm/atomic: do not branch based on the value of current->comm[0]  
Date: Sat, 5 Nov 2022 23:20:12 +0100 [thread overview]  
Message-ID: <20221105222012.4226-1-Jason@zx2c4.com> (raw)

This reverts 26b1d3b527e7 ("drm/atomic: Take the atomic toys away from X"), a rootkit-like kludge that has no business being inside of a general purpose kernel. It's the type of debugging hack I'll use momentarily but never commit, or a sort of babbies-first-process-hider malware trick.

The backstory is that some userspace code -- xorg-server -- has a modesetting DDX that isn't really coded right. With nobody wanting to maintain X11 anymore, rather than fixing the buggy code, the kernel was adjusted to avoid having to touch X11. A bummer, but fair enough: if the kernel doesn't want to support some userspace API any more, the right thing to do is to arrange for a graceful fallback where userspace thinks it's not available in a manageable way.

However, the *way* it goes about doing that is just to check `current->comm[0] == 'X'`, and disable it for only that case. So that means it's *not* simply a matter of the kernel not wanting to support a particular userspace API anymore, but rather it's the kernel not wanting to support xorg-server, in theory, but actually, it turns out, that's all processes that begin with 'X'.

Playing games with `current->comm` like this is obviously wrong, and it's pretty shocking that this ever got committed.

Fortunately, since this was committed, somebody did actually disable the userspace side by default in X11: [https://gitlab.freedesktop.org/xorg/xserver/-/merge\\_requests/180](https://gitlab.freedesktop.org/xorg/xserver/-/merge_requests/180) and this was three years ago. So userspace is mostly fine now for ordinary default usage. And people who opt into this -- since it does actually work fine for many use cases on i915 -- ostensibly know what they're getting themselves into (my case).

So let's just revert this `comm[0] == 'X'` business entirely, but still allow for `value == 2`, in case anybody actually started working on that part elsewhere.

Fixes: 26b1d3b527e7 ("drm/atomic: Take the atomic toys away from X")

Cc: Daniel Vetter <daniel.vetter@intel.com>  
Cc: Peter Zijlstra <peterz@infradead.org>  
Cc: Ilia Mirkin <imirkin@alum.mit.edu>  
Cc: Maarten Lankhorst <maarten.lankhorst@linux.intel.com>  
Cc: Nicholas Kazlauskas <nicholas.kazlauskas@amd.com>  
Cc: Christian Brauner <brauner@kernel.org>  
Cc: Michel Dänzer <michel@daenzer.net>  
Cc: Alex Deucher <alexdeucher@gmail.com>

Cc: Adam Jackson <ajax@redhat.com>  
Cc: Greg Kroah-Hartman <gregkh@linuxfoundation.org>  
Cc: Sean Paul <sean@poorly.run>  
Cc: David Airlie <airlied@linux.ie>  
Cc: Rob Clark <robdclark@gmail.com>  
Cc: Sultan Alsawaf <sultan@kerneltoast.com>  
Signed-off-by: Jason A. Donenfeld <Jason@zx2c4.com>

---  
drivers/gpu/drm/drm\_ioctl.c | 5 -----  
1 file changed, 5 deletions(-)

```
diff --git a/drivers/gpu/drm/drm_ioctl.c b/drivers/gpu/drm/drm_ioctl.c
index ca2a6e6101dc..017f31e67179 100644
--- a/drivers/gpu/drm/drm_ioctl.c
+++ b/drivers/gpu/drm/drm_ioctl.c
@@ -336,11 +336,6 @@ drm_setclientcap(struct drm_device *dev, void *data, struct drm_file *file_priv)
     case DRM_CLIENT_CAP_ATOMIC:
         if (!drm_core_check_feature(dev, DRIVER_ATOMIC))
             return -EOPNOTSUPP;
-        /* The modesetting DDX has a totally broken idea of atomic. */
-        if (current->comm[0] == 'X' && req->value == 1) {
-            pr_info("broken atomic modeset userspace detected, disabling atomic\n");
-            return -EOPNOTSUPP;
-        }
         if (req->value > 2)
             return -EINVAL;
         file_priv->atomic = req->value;
--
2.38.1
```

---

[reply](#) [other threads](#): [~2022-11-05 22:21 UTC|newest]

**Thread overview:** [no followups] [expand](#)[flat|nested] [mbox.gz](#) [Atom feed](#)

find likely ancestor, descendant, or conflicting patches for [this message](#):

[\(help\)](#)

---

### Reply instructions:

You may reply publicly to [this message](#) via plain-text email using any one of the following methods:

\* Save the following mbox file, import it into your mail client, and reply-to-all from there: [mbox](#)

Avoid top-posting and favor interleaved quoting:  
[https://en.wikipedia.org/wiki/Posting\\_style#Interleaved\\_style](https://en.wikipedia.org/wiki/Posting_style#Interleaved_style)

\* Reply using the `--to`, `--cc`, and `--in-reply-to` switches of `git-send-email(1)`:

```
git send-email \
  --in-reply-to=20221105222012.4226-1-Jason@zx2c4.com \
  --to=jason@zx2c4.com \
  --cc=airlied@linux.ie \
  --cc=ajax@redhat.com \
  --cc=alexdeucher@gmail.com \
  --cc=brauner@kernel.org \
  --cc=daniel.vetter@intel.com \
  --cc=dri-devel@lists.freedesktop.org \
  --cc=gregkh@linuxfoundation.org \
  --cc=imirkin@alum.mit.edu \
  --cc=linux-api@vger.kernel.org \
  --cc=linux-kernel@vger.kernel.org \
  --cc=maarten.lankhorst@linux.intel.com \
```

--cc=michel@daenzer.net \  
--cc=nicholas.kazlauskas@amd.com \  
--cc=peterz@infradead.org \  
--cc=robdclark@gmail.com \  
--cc=sean@poorly.run \  
--cc=sultan@kerneltoast.com \  
/path/to/YOUR\_REPLY

<https://kernel.org/pub/software/scm/git/docs/git-send-email.html>

\* If your mail client supports setting the **In-Reply-To** header  
via mailto: links, try the [mailto: link](#)

Be sure your reply has a **Subject:** header at the top and a blank line before the message body.

---

This is a public inbox, see [mirroring instructions](#)  
for how to clone and mirror all data and code used for this inbox;  
as well as URLs for NNTP newsgroup(s).