
Subject: [PATCH] Fix UTS corruption during clone(CLONE_NEWUTS)

Posted by [Alexey Dobriyan](#) on Fri, 14 Sep 2007 14:57:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

struct utsname is copied from master one without any exclusion.

Here is sample output from one proggie doing

```
sethostname("aaaaaaaaaaaaaaaaaaaaaaaaaaaaa");
sethostname("bbbbbbbbbbbbbbbbbbbbbbbbbbbbbb");
```

and another

```
clone(, CLONE_NEWUTS, ...)
uname()
```

```
hostname = 'aaaaaaaaaaaaaaaaaaaaaaaaabbbb'
hostname = 'bbbaaaaaaaaaaaaaaaaaaaaaaaaaa'
hostname = 'aaaaaaaabbbbbbbbbbbbbbbbbbbb'
hostname = 'aaaaaaaaaaaaaaaaaaaaaaaaabbbb'
hostname = 'aaaaaaaaaaaaaaaaaaaaaaaaaabb'
hostname = 'aaabbbbbbbbbbbbbbbbbbbbbbbb'
hostname = 'bbbbbbbbbbbbbbbbbaaaaaaaaaaaaa'
```

Hostname is sometimes corrupted.

Yes, even _the_ simplest namespace activity had bug in it. :-(

Signed-off-by: Alexey Dobriyan <adobriyan@sw.ru>

```
kernel/utsname.c | 2 ++
1 file changed, 2 insertions(+)
```

--- a/kernel/utsname.c

+++ b/kernel/utsname.c

```
@@ -28,7 +28,9 @@ static struct uts_namespace *clone_uts_ns(struct uts_namespace *old_ns)
    if (!ns)
        return ERR_PTR(-ENOMEM);
```

```
+ down_read(&uts_sem);
    memcpy(&ns->name, &old_ns->name, sizeof(ns->name));
+ up_read(&uts_sem);
    kref_init(&ns->kref);
    return ns;
}
```
