
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 = 'bbbaaaaaaaaaaaaaaaaaaaaaaaaa'
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;
}
```

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

Posted by [serge](#) on Fri, 14 Sep 2007 20:02:15 GMT

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

Quoting Alexey Dobriyan (adobriyan@sw.ru):

> struct utsname is copied from master one without any exclusion.

>

> Here is sample output from one proggy doing

>

> sethostname("aaaaaaaaaaaaaaaaaaaaaaaaaaaaa");

> sethostname("bbbbbbbbbbbbbbbbbbbbbbbbbbbbbb");

>

> and another

>

> clone(., CLONE_NEWUTS, ...)

> uname()

>

>

> hostname = 'aaaaaaaaaaaaaaaaaaaaaaaaabbbb'

> hostname = 'bbbaaaaaaaaaaaaaaaaaaaaaaaaa'

> hostname = 'aaaaaaaabbbbbbbbbbbbbbbbbbbb'

> hostname = 'aaaaaaaaaaaaaaaaaaaaaaaaabbbb'

> hostname = 'aaaaaaaaaaaaaaaaaaaaaaaaabb'

> hostname = 'aaabbbbbbbbbbbbbbbbbbbbbbbb'

> hostname = 'bbbbbbbbbbbbbbbbbaaaaaaaaaaaa'

>

> Hostname is sometimes corrupted.

>

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

>

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

picking my jaw up off the floor just long enough to type

Signed-off-by: Serge Hallyn <serue@us.ibm.com>

and limp away in shame

thanks Alexey,

-serge

> ---

>

> 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;
> }
>
> -
> To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
> the body of a message to 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/
```
