
Subject: Re: [PATCH] create_new_namespaces: fix improper return of NULL

Posted by [Cedric Le Goater](#) on Tue, 19 Jun 2007 14:05:00 GMT

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

Oleg Nesterov wrote:

> Untested.

>

> dup_mnt_ns() and clone_uts_ns() return NULL on failure. This is wrong,

> create_new_namespaces() uses ERR_PTR() to catch an error. This means

> that the subsequent create_new_namespaces() will hit BUG_ON() in

> copy_mnt_ns() or copy_utsname().

I sent one just like it :

<http://lkml.org/lkml/2007/6/12/142>

but your changelog is worth adding. much better than mine.

thanks,

C.

> Signed-off-by: Oleg Nesterov <oleg@tv-sign.ru>

>

> --- ns/fs/namespace.c~1_NS_NULL 2007-05-21 13:57:56.000000000 +0400

> +++ ns/fs/namespace.c 2007-06-19 17:26:35.000000000 +0400

> @@ -1457,7 +1457,7 @@ static struct mnt_namespace *dup_mnt_ns(
>

>

> new_ns = kmalloc(sizeof(struct mnt_namespace), GFP_KERNEL);

> if (!new_ns)

> - return NULL;

> + return ERR_PTR(-ENOMEM);

>

> atomic_set(&new_ns->count, 1);

> INIT_LIST_HEAD(&new_ns->list);

> @@ -1471,7 +1471,7 @@ static struct mnt_namespace *dup_mnt_ns(
>

> if (!new_ns->root) {

> up_write(&namespace_sem);

> kfree(new_ns);

> - return NULL;

> + return ERR_PTR(-ENOMEM);

> }

> spin_lock(&vfsmount_lock);

> list_add_tail(&new_ns->list, &new_ns->root->mnt_list);

> --- ns/kernel/utsname.c~1_NS_NULL 2007-05-21 13:57:59.000000000 +0400

> +++ ns/kernel/utsname.c 2007-06-19 17:35:22.000000000 +0400

> @@ -13,6 +13,7 @@

> #include <linux/uts.h>

```

> #include <linux/utsname.h>
> #include <linux/version.h>
> +#include <linux/err.h>
>
> /*
>  * Clone a new ns copying an original utsname, setting refcount to 1
> @@ -24,10 +25,11 @@ static struct uts_namespace *clone_uts_n
>  struct uts_namespace *ns;
>
>  ns = kmalloc(sizeof(struct uts_namespace), GFP_KERNEL);
> - if (ns) {
> - memcpy(&ns->name, &old_ns->name, sizeof(ns->name));
> - kref_init(&ns->kref);
> - }
> + if (!ns)
> + return ERR_PTR(-ENOMEM);
> +
> + memcpy(&ns->name, &old_ns->name, sizeof(ns->name));
> + kref_init(&ns->kref);
>  return ns;
> }
>
>
>

```

Containers mailing list
Containers@lists.linux-foundation.org
<https://lists.linux-foundation.org/mailman/listinfo/containers>

Subject: Re: [PATCH] create_new_namespaces: fix improper return of NULL
Posted by [Oleg Nesterov](#) on Tue, 19 Jun 2007 14:27:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

On 06/19, Cedric Le Goater wrote:

```

>
> Oleg Nesterov wrote:
> > Untested.
> >
> > dup_mnt_ns() and clone_uts_ns() return NULL on failure. This is wrong,
> > create_new_namespaces() uses ERR_PTR() to catch an error. This means
> > that the subsequent create_new_namespaces() will hit BUG_ON() in
> > copy_mnt_ns() or copy_utsname().
>
> I sent one just like it :
>
> http://lkml.org/lkml/2007/6/12/142

```

Ah, thanks.

Your patch is more complete, it also fixes kernel/user_namespace.c (which I don't see in 2.6.22-rc5). I don't think this fix is urgent, so...

Andrew, please ignore this patch.

Oleg.

Containers mailing list
Containers@lists.linux-foundation.org
<https://lists.linux-foundation.org/mailman/listinfo/containers>
