Subject: [PATCH] create_new_namespaces: fix improper return of NULL
Posted by Oleg Nesterov on Tue, 19 Jun 2007 13:51:29 GMT
View Forum Message <> Reply to Message

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().

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