Subject: [PATCH] sys_getsid/sys_getpgid return wrong id for task from another ns
Posted by Pavel Emelianov on Fri, 24 Aug 2007 08:41:10 GMT
View Forum Message <> Reply to Message

When calling the sys_getsid/sys_getpgid for task, that actually
lives in another namespace (sub-namespace) the return value should
be not the id as this task sees it, but the id as the caller does.

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

---

 kernel/sys.c | 18 ++++++++++--------
 1 files changed, 10 insertions(+), 8 deletions(-)

```
diff --git a/kernel/sys.c b/kernel/sys.c
index c7c4fa4..c827186 100644
--- a/kernel/sys.c
+++ b/kernel/sys.c
@@ -993,16 +995,17 @@ asmlinkage long sys_getpgid(pid_t pid)
  else {
   int retval;
   struct task_struct *p;
+  struct pid_namespace *ns;

-  read_lock(&tasklist_lock);
-  p = find_task_by_pid_ns(pid,
-    current->nsproxy->pid_ns);
+  ns = current->nsproxy->pid_ns;

+  read_lock(&tasklist_lock);
+  p = find_task_by_pid_ns(pid, ns);
   retval = -ESRCH;
   if (p) {
    retval = security_task_getpgid(p);
    if (!retval)
-    retval = task_pgrp_vnr(p);
+    retval = task_pgrp_nr_ns(p, ns);
   }
   read_unlock(&tasklist_lock);
   return retval;
@@ -1026,16 +1029,17 @@ asmlinkage long sys_getsid(pid_t pid)
  else {
   int retval;
   struct task_struct *p;
+  struct pid_namespace *ns;

-  read_lock(&tasklist_lock);
```

```
-  p = find_task_by_pid_ns(pid,
-    current->nsproxy->pid_ns);
+  ns = current->nsproxy->pid_ns;

+  read_lock(&tasklist_lock);
+  p = find_task_by_pid_ns(pid, ns);
   retval = -ESRCH;
   if (p) {
    retval = security_task_getsid(p);
    if (!retval)
-    retval = task_session_vnr(p);
+    retval = task_session_nr_ns(p, ns);
   }
   read_unlock(&tasklist_lock);
   return retval;
```

_____

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