
Subject: Fw: Re: [PATCH] Fix capability.c to work with threaded init
Posted by [Sukadev Bhattiprolu](#) on Tue, 07 Aug 2007 21:31:32 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi Pavel,

This patch seems to be missing from your most recent patchset.
Do you want to include it in the set as a helper or should I
just send this to Andrew separately ?

Suka

----- Forwarded message from sukadev@us.ibm.com -----

| Date: Fri, 3 Aug 2007 13:51:20 -0700
| From: sukadev@us.ibm.com
| To: Oleg Nesterov <oleg@tv-sign.ru>
| Cc: Containers <containers@lists.osdl.org>, Pavel Emelianov <xemul@openvz.org>
| Subject: Re: [PATCH] Fix capability.c to work with threaded init

| Oleg Nesterov [oleg@tv-sign.ru] wrote:
| | On 08/03, Dave Hansen wrote:
| | >
| | > On Thu, 2007-08-02 at 23:26 -0700, sukadev@us.ibm.com wrote:
| | > >
| | > > Callers of is_container_init() should pass in task->group_leader
| | > > to ensure they work with threaded-init.
| | >
| | > Can you explain this in a little more detail? That's a pretty sparse
| | > changelog.

| You are right. The changelog could be better. How about this:

| | Without this change cap_set_all() skips only the main thread of /sbin/init,
| | but we should skip the entire process as the comment states.

| | Oleg.

| ---

| From: Sukadev Bhattiprolu <sukadev@us.ibm.com>
| Subject: [PATCH] cap_set_all() must skip all threads of init

| When setting capabilities, cap_set_all() must skip all threads of the
| container_init process - not just the main thread.

Signed-off-by: Sukadev Bhattiprolu <sukadev@us.ibm.com>

kernel/capability.c | 2 +-
1 file changed, 1 insertion(+), 1 deletion(-)

Index: lx26-23-rc1-mm1/kernel/capability.c

=====

--- lx26-23-rc1-mm1.orig/kernel/capability.c 2007-08-02 22:58:02.000000000 -0700

+++ lx26-23-rc1-mm1/kernel/capability.c 2007-08-02 22:58:17.000000000 -0700

@@ -137,7 +137,7 @@ static inline int cap_set_all(kernel_cap
int found = 0;

do_each_thread(g, target) {
- if (target == current || is_container_init(target))
+ if (target == current || is_container_init(target->group_leader))
continue;
found = 1;
if (security_capset_check(target, effective, inheritable,

Containers mailing list

Containers@lists.linux-foundation.org

<https://lists.linux-foundation.org/mailman/listinfo/containers>

----- End forwarded message -----

Containers mailing list

Containers@lists.linux-foundation.org

<https://lists.linux-foundation.org/mailman/listinfo/containers>
