Subject: [PATCH 1/1] user namespace: fix copy_user_ns return value
Posted by serue on Tue, 17 Jul 2007 19:33:27 GMT
View Forum Message <> Reply to Message

>From 32f86740d27ef77160e438cd7dc4fcd5df159dd0 Mon Sep 17 00:00:00 2001
From: Serge E. Hallyn <serue@us.ibm.com>
Date: Tue, 17 Jul 2007 15:28:17 -0400
Subject: [PATCH 1/1] user namespace: fix copy_user_ns return value

When a CONFIG_USER_NS=n and a user tries to unshare some
namespace other than the user namespace, the dummy
copy_user_ns returns NULL rather than the old_ns. This
value then gets assigned to task->nsproxy->user_ns, so
that a subsequent setuid, which uses task->nsproxy->user_ns,
causes a NULL pointer deref.

Fix this by returning old_ns.

I believe this is a bug both in -mm and mainline.

Signed-off-by: Serge E. Hallyn <serue@us.ibm.com>
---
 include/linux/user_namespace.h | 2 +-
 1 files changed, 1 insertions(+), 1 deletions(-)

diff --git a/include/linux/user_namespace.h b/include/linux/user_namespace.h
index bb32057..1101b0c 100644
--- a/include/linux/user_namespace.h
+++ b/include/linux/user_namespace.h
@@ -49,7 +49,7 @@ static inline struct user_namespace *copy_user_ns(int flags,
 if (flags & CLONE_NEWUSER)
 return ERR_PTR(-EINVAL);

- return NULL;
+ return old_ns;
 }

 static inline void put_user_ns(struct user_namespace *ns)
--
1.5.1.1.GIT

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