
Subject: [RFC] [PATCH -mm] agp: remove uid comparison as security check
Posted by [serue](#) on Wed, 12 Dec 2007 20:57:05 GMT

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

>From d4ca1a9749c5b40325ec2db9fcde2f2cbd0e0978 Mon Sep 17 00:00:00 2001
From: serue@us.ibm.com <serue@us.ibm.com>
Date: Wed, 5 Dec 2007 13:55:36 -0800
Subject: [RFC] [PATCH -mm] agp: remove uid comparison as security check

In the face of containers and user namespaces, a uid==0 check for security is not safe. Switch to a capability check.

I'm not sure I picked the right capability, but this being AGP CAP_SYS_RAWIO seemed to make sense.

Signed-off-by: Serge Hallyn <serue@us.ibm.com>

drivers/char/agp/frontend.c | 2 +-
1 files changed, 1 insertions(+), 1 deletions(-)

diff --git a/drivers/char/agp/frontend.c b/drivers/char/agp/frontend.c
index 9bd5a95..55d7a82 100644

--- a/drivers/char/agp/frontend.c

+++ b/drivers/char/agp/frontend.c

@@ -689,7 +689,7 @@ static int agp_open(struct inode *inode, struct file *file)
set_bit(AGP_FF_ALLOW_CLIENT, &priv->access_flags);
priv->my_pid = current->pid;

- if ((current->uid == 0) || (current->suid == 0)) {
+ if (capable(CAP_SYS_RAWIO)) {
/* Root priv, can be controller */
set_bit(AGP_FF_ALLOW_CONTROLLER, &priv->access_flags);
}
--

1.5.1

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