
Subject: [RFC] [PATCH 4/8] user namespace: enforce CAP_NS_OVERRIDE for cross-namespace kill

Posted by [serue](#) on Fri, 07 Dec 2007 19:14:26 GMT

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

>From 62e6efe435a24f430e28f2398f374cef197b4964 Mon Sep 17 00:00:00 2001

From: sergeh@us.ibm.com <sergeh@us.ibm.com>

Date: Thu, 29 Nov 2007 08:18:16 -0800

Subject: [RFC] [PATCH 4/8] user namespace: enforce CAP_NS_OVERRIDE for cross-namespace kill

Require CAP_NS_OVERRIDE to 'kill' across user namespaces.

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

kernel/signal.c | 5 +++++

1 files changed, 5 insertions(+), 0 deletions(-)

diff --git a/kernel/signal.c b/kernel/signal.c

index 787521e..a06dcc2 100644

--- a/kernel/signal.c

+++ b/kernel/signal.c

@@ -534,6 +534,11 @@ static int check_kill_permission(int sig, struct siginfo *info,
error = audit_signal_info(sig, t); /* Let audit system see the signal */

if (error)

return error;

+

+ if (current->nsproxy->user_ns != t->nsproxy->user_ns

+ && !(capable(CAP_KILL) && capable(CAP_NS_OVERRIDE)))

+ return -EPERM;

+

error = -EPERM;

if (((sig != SIGCONT) ||

(task_session_nr(current) != task_session_nr(t)))

--

1.5.1

Containers mailing list

Containers@lists.linux-foundation.org

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