
Subject: Re: [PATCH 2/2] hijack: update task_alloc_security
Posted by [Crispin Cowan](#) on Wed, 28 Nov 2007 05:50:00 GMT
[View Forum Message](#) <> [Reply to Message](#)

Serge E. Hallyn wrote:

> Quoting Stephen Smalley (sds@tycho.nsa.gov):

>

>> I agree with this part - we don't want people to have to choose between
>> using containers and using selinux, so if hijack is going to be a
>> requirement for effective use of containers, then we need to make them
>> work together.

>>

> Absolutely, we just need to decide how to properly make it work with

> selinux. Maybe we check for

>

> allow (current_domain):(hijacked_process_domain) hijack

> type_transition hijacked_process_domain \

> vserver_enter_binary_t:process vserver1_hijack_admin_t;

>

Is there to be an LSM hook, so that modules can decide on an arbitrary
decision of whether to allow a hijack? So that this "do the right
SELinux" thing can be generalized for all LSMs to do the right thing.

Crispin

--

Crispin Cowan, Ph.D. <http://crispincowan.com/~crispin>

CEO, Mercenary Linux <http://mercenarylinux.com/>

Itanium. Vista. GPLv3. Complexity at work

Containers mailing list

Containers@lists.linux-foundation.org

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