

## SELinux - Bug #7178

### Allow passenger\_t to EXECMEM

08/20/2014 11:17 AM - Lukas Zapletal

<b>Status:</b> Closed	
<b>Priority:</b> High	
<b>Assignee:</b> Lukas Zapletal	
<b>Category:</b> Packaging	
<b>Target version:</b> 1.7.0	
<b>Difficulty:</b> trivial	<b>Fixed in Releases:</b>
<b>Triaged:</b>	<b>Found in Releases:</b>
<b>Bugzilla link:</b> 1112607	<b>Red Hat JIRA:</b>
<b>Pull request:</b> <a href="https://github.com/foreman/foreman-selinux/pull/32">https://github.com/foreman/foreman-selinux/pull/32</a>	
<b>Description</b>	
It was confirmed by our QA department that our application does work file in Enforcing.	
<b>Related issues:</b>	
Related to SELinux - Tracker #7249: Policy with workarounds for Foreman w/ Ka...	<b>Closed</b> <b>08/25/2014</b>

#### Associated revisions

##### Revision d867377e - 08/20/2014 04:45 PM - Lukas Zapletal

Fixes #7178 - allowed passenger\_t to execmem

Foreman-tasks wont start on RHEL7

##### Revision d5e80cf1 - 08/20/2014 04:47 PM - Lukas Zapletal

Merge pull request #28 from lzap/execmem-7178

Fixes #7178 - allowed passenger\_t to execmem

##### Revision e86bf009 - 09/26/2014 08:20 AM - Lukas Zapletal

Refs #7178 - removed passenger\_t execmem rule

This reverts commit d867377e56451fc43030a30958499d34e6f4e485.

#### History

##### #1 - 08/20/2014 04:36 PM - Lukas Zapletal

- Subject changed from *Don't audit passenger's EXECMEM* to *Allos passenger\_t to EXECMEM*

Scratch that for RHEL7, after investigation from this evening with Jason and Og, it turns out it is not passenger but foreman-tasks what causes this denial. And it does not start without this.

We run foreman-tasks (dynflow process) in passenger\_t because it boots whole foreman to do its work. We need to allow this rule.

It does work in RHEL6 but in RHEL7 it does not start. Permissive only gives this denial and enforcing stops tasks from coming up. Allowing this rule proceeds.

```
service foreman-tasks start
Redirecting to /bin/systemctl start foreman-tasks.service
Job for foreman-tasks.service failed. See 'systemctl status foreman-tasks.service' and 'journalctl -xn' for de
tails.
[root@el7-smoketest ~]# vi log
[root@el7-smoketest ~]# audit2allow -m passenger-execmem < log

module passenger-execmem 1.0;

require {
    type passenger_t;
    class process execmem;
```

```

}

#===== passenger_t =====
allow passenger_t self:process execmem;
You have new mail in /var/spool/mail/root
[root@el7-smoketest ~]# audit2allow -M passenger-execmem < log
***** IMPORTANT *****
To make this policy package active, execute:

semodule -i passenger-execmem.pp

[root@el7-smoketest ~]# semodule -i passenger-execmem.pp
[root@el7-smoketest ~]# getenforce
Enforcing
[root@el7-smoketest ~]# service foreman-tasks start
Redirecting to /bin/systemctl start foreman-tasks.service
You have new mail in /var/spool/mail/root
[root@el7-smoketest ~]# cat log
type=AVC msg=audit(1408565585.751:711): avc: denied { execmem } for pid=52386 comm="ruby" scontext=system_u
:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
[root@el7-smoketest ~]# systemctl status foreman-tasks
foreman-tasks.service - Foreman jobs daemon
   Loaded: loaded (/usr/lib/systemd/system/foreman-tasks.service; enabled)
   Active: active (running) since Wed 2014-08-20 16:22:15 EDT; 22s ago
     Docs: https://github.com/iNecas/foreman-tasks
  Process: 52738 ExecStop=/usr/bin/foreman-tasks stop (code=exited, status=134)
  Process: 54593 ExecStart=/usr/bin/foreman-tasks start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/foreman-tasks.service
           └─54635 dynflow_executor
             └─54637 dynflow_executor_monitor

Aug 20 16:20:56 el7-smoketest.sat6.lab.eng.bos.redhat.com foreman-tasks[54593]: ...
Aug 20 16:20:59 el7-smoketest.sat6.lab.eng.bos.redhat.com foreman-tasks[54593]: ...
Aug 20 16:20:59 el7-smoketest.sat6.lab.eng.bos.redhat.com foreman-tasks[54593]: ...
Aug 20 16:22:14 el7-smoketest.sat6.lab.eng.bos.redhat.com foreman-tasks[54593]: ...
Aug 20 16:22:15 el7-smoketest.sat6.lab.eng.bos.redhat.com systemd[1]: Started Fo...
Hint: Some lines were ellipsized, use -l to show in full.

```

## #2 - 08/20/2014 05:01 PM - Anonymous

- Status changed from Assigned to Closed
- % Done changed from 10 to 100

Applied in changeset [d867377e56451fc43030a30958499d34e6f4e485](#).

## #3 - 08/21/2014 03:37 AM - Dominic Cleal

- translation missing: en.field\_release set to 21

## #4 - 08/21/2014 06:21 AM - Lukas Zapletal

- Subject changed from Allos passenger\_t to EXECMEM to Allow passenger\_t to EXECMEM

Investigating if daemons gem (used by foreman-tasks) does not cause that.

## #5 - 08/25/2014 01:14 PM - Lukas Zapletal

- Related to Tracker #7249: Policy with workarounds for Foreman w/ Katello added

## #6 - 09/26/2014 04:42 AM - The Foreman Bot

- Pull request <https://github.com/theforeman/foreman-selinux/pull/32> added
- Pull request deleted ()