SELinux - Bug #6013

AVC denials from Passenger on Foreman 1.6 on EL7

06/02/2014 03:28 PM - Dominic Cleal

Status:	Closed		
Priority:	Normal		
Assignee:	Lukas Zapletal		
Category:			
Target version:	1.6.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

foreman-selinux-1.6.0-0.develop.201405301314git8ad6a63.el7.noarch
redhat-release-server-7.0-0.5.el7.x86_64
selinux-policy-3.12.1-153.el7.noarch
selinux-policy-targeted-3.12.1-153.el7.noarch

This seems to block Passenger from starting at all:

```
type=AVC msg=audit(1401722952.037:191): avc:  denied  { getattr } for  pid=6721 comm="rm" name="/"
 dev="vda1" ino=128 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:fs_t:s0 t
class=filesystem
type=SYSCALL msg=audit(1401722952.037:191): arch=c000003e syscall=138 success=no exit=-13 a0=5 a1=
7fff87ae31d0 a2=78e730 a3=7fff87ae2f80 items=0 ppid=6390 pid=6721 auid=4294967295 uid=0 gid=0 euid
=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="rm" exe="/usr/bin/rm" subj
=system_u:system_r:passenger_t:s0 key=(null)

require {
    type passenger_t;
}

#============= passenger_t ==============
fs_getattr_xattr_fs(passenger_t)
```

or without macros...

```
require {
    type passenger_t;
    type fs_t;
    class filesystem getattr;
}

#============= passenger_t ==============
allow passenger_t fs_t:filesystem getattr;

type=AVC msg=audit(1401722832.531:183): avc:  denied  { block_suspend } for  pid=6402 comm="Passen
gerHelper" capability=36  scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:pas
senger_t:s0 tclass=capability2
type=SYSCALL msg=audit(1401722832.531:183): arch=c000003e syscall=233 success=yes exit=0 a0=9 a1=2
 a2=100000014 a3=1701950 items=0 ppid=6390 pid=6402 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsui
d=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="PassengerHelper" exe="/usr/lib64/gems/ru
by/passenger-4.0.18/agents/PassengerHelperAgent" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1401722832.531:183): avc:  denied  { block_suspend } for  pid=6402 comm="Passen
gerHelper" capability=36  scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:pas
senger_t:s0 tclass=capability2
type=SYSCALL msg=audit(1401722832.531:183): arch=c000003e syscall=233 success=yes exit=0 a0=9 a1=2
 a2=100000014 a3=1701950 items=0 ppid=6390 pid=6402 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsui
d=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="PassengerHelper" exe="/usr/lib64/gems/ru
```

```
by/passenger-4.0.18/agents/PassengerHelperAgent" subj=system_u:system_r:passenger_t:s0 key=(null)

require {
    type passenger_t;
    class capability2 block_suspend;
}

#============= passenger_t ==============
allow passenger_t self:capability2 block_suspend;
```

Related issues:

Related to SELinux - Bug #6014: AVC denials from Puppet under Passenger on Fo...	**Closed**	**06/02/2014**
Blocks Foreman - Tracker #4447: Support installation on RHEL 7	**Closed**	**02/25/2014**

Associated revisions

Revision 7a59c903 - 08/12/2014 10:11 AM - Lukas Zapletal

Fixes #6013, #6014, #6979 - changes for RHEL7

History

#1 - 06/02/2014 03:31 PM - Dominic Cleal

- Description updated

#2 - 06/02/2014 03:34 PM - Dominic Cleal

- Blocks Tracker #4447: Support installation on RHEL 7 added

#3 - 06/02/2014 03:34 PM - Dominic Cleal

- Related to Bug #6014: AVC denials from Puppet under Passenger on Foreman 1.6 on EL7 added

#4 - 06/06/2014 09:51 AM - Dominic Cleal

- translation missing: en.field_release set to 10

#5 - 07/30/2014 09:12 AM - Ohad Levy

- Target version set to 1.7.5

#6 - 08/07/2014 09:52 AM - Lukas Zapletal

- Status changed from New to Ready For Testing

- Assignee set to Lukas Zapletal

For the fs_getattr_xattr_fs, I was able to track it down a bit. Passenger creates few directories under /tmp during startup and then removes whole trees. These are /tmp/PassengerTeeInput-0.17364735999858316 and /tmp/passenger.1.0.32502/generation-1/backends/. They use "rm" to remove directories recursively and this process somehow compares attributes.

I've no idea for the block_suspend, allowed too, let's see the review.

https://github.com/theforeman/foreman-selinux/pull/26

#7 - 08/12/2014 11:01 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 7a59c90304ef32a67457a8071bbda07d161b6236.