SELinux - Bug #4458

AVC denials aboutname="online" dev=sysfs ino=23 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:sysfs_t:s0 tclass=file

02/26/2014 08:37 AM - Jan Pazdziora

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

Description

Installing Foreman nightly from

```
baseurl=http://yum.theforeman.org/nightly/el6/$basearch
```

on RHEL 6.5 causes AVC denials to eventually show up in the audit.log:

```
type=AVC msg=audit(1393403231.005:232): avc:  denied  { search } for  pid=23349 comm="ps" name="/"
 dev=sysfs ino=1 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:sysfs_t:
s0 tclass=dir
type=AVC msg=audit(1393403231.005:232): avc:  denied  { read } for  pid=23349 comm="ps" name="onli
ne" dev=sysfs ino=23 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:sysf
s_t:s0 tclass=file
type=AVC msg=audit(1393403231.005:232): avc:  denied  { open } for  pid=23349 comm="ps" name="onli
ne" dev=sysfs ino=23 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:sysf
s_t:s0 tclass=file
type=AVC msg=audit(1393403409.342:248): avc:  denied  { search } for  pid=23695 comm="PassengerHel
per" name="/" dev=sysfs ino=1 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:obje
ct_r:sysfs_t:s0 tclass=dir
type=AVC msg=audit(1393403409.342:248): avc:  denied  { read } for  pid=23695 comm="PassengerHelpe
r" name="online" dev=sysfs ino=23 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:
object_r:sysfs_t:s0 tclass=file
type=AVC msg=audit(1393403409.342:248): avc:  denied  { open } for  pid=23695 comm="PassengerHelpe
r" name="online" dev=sysfs ino=23 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:
object_r:sysfs_t:s0 tclass=file
```

The file (path) in question is /sys/devices/system/cpu/online.

Related issues:

Is duplicate of SELinux - Bug #3465: AVC denials with Foreman 1.3 on RHEL 6	**Closed**	**10/22/2013**

History

#1 - 02/26/2014 08:41 AM - Lukas Zapletal

- Category set to 56

Thanks. It looks like we need to open access to sysfs domain, but I can't find WHY it tries to read this file.

It looks like both agent and memory-stats processes are using "ps" tool to get some info about CPU:

https://github.com/phusion/passenger/blob/master/ext/common/Utils/ProcessMetricsCollector.h#L474

https://github.com/phusion/passenger/blob/master/lib/phusion_passenger/admin_tools/memory_stats.rb#L217-L278

But I don't see any leaked descriptors or anything like that (when I run it manually):

```
open("/sys/devices/system/cpu/online", O_RDONLY|O_CLOEXEC) = 3
```

```
read(3, "0-3\n", 8192)                  = 4
close(3)                                = 0
```

#2 - 02/26/2014 08:46 AM - Dominic Cleal

- Is duplicate of Bug #3465: AVC denials with Foreman 1.3 on RHEL 6 added

#3 - 02/26/2014 08:46 AM - Dominic Cleal

- Project changed from Foreman to SELinux

- Category deleted (56)

- Status changed from New to Duplicate

Looks the same as #3465.

#4 - 02/26/2014 08:51 AM - Lukas Zapletal

Ok I guess we need to add the following rules:

```
allow passenger_t sysfs_t:dir search;
allow passenger_t sysfs_t:file { read open };
```