SELinux - Bug #2789

SELinux denials in 1.2

07/15/2013 05:39 AM - Lukas Zapletal

Status:	Closed		
Priority:	Normal		
Assignee:	Lukas Zapletal		
Category:			
Target version:	1.2.1		
Difficulty:	easy	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

We have couple of denials in the 1.2 release.

First bunch reported by Yaniv Kaul:

```
type=AVC msg=audit(1373816913.310:17): avc:  denied  { setattr } for
 pid=1303 comm="ruby"
name="foreman.xiolab.lab.abc.com.yaml20130714-1303-131hr6b-0" dev=dm-0
ino=792378 scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:var_lib_t:s0 tclass=file
type=AVC msg=audit(1373816913.320:18): avc:  denied  { rename } for
 pid=1303 comm="ruby"
name="foreman.xiolab.lab.abc.com.yaml20130714-1303-131hr6b-0" dev=dm-0
ino=792378 scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:var_lib_t:s0 tclass=file
type=AVC msg=audit(1373816913.320:18): avc:  denied  { unlink } for
 pid=1303 comm="ruby" name="foreman.xiolab.lab.abc.com.yaml" dev=dm-0
ino=792350 scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:var_lib_t:s0 tclass=file
type=AVC msg=audit(1373816913.949:19): avc:  denied  { getattr } for
 pid=1303 comm="ruby" path="/sbin/ifconfig" dev=dm-0 ino=44
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:ifconfig_exec_t:s0 tclass=file
type=AVC msg=audit(1373816913.949:20): avc:  denied  { execute } for
 pid=1303 comm="ruby" name="ifconfig" dev=dm-0 ino=44
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:ifconfig_exec_t:s0 tclass=file
type=AVC msg=audit(1373816913.953:21): avc:  denied  { read open } for
 pid=1416 comm="sh" name="ifconfig" dev=dm-0 ino=44
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:ifconfig_exec_t:s0 tclass=file
type=AVC msg=audit(1373816913.953:21): avc:  denied  { execute_no_trans }
for  pid=1416 comm="sh" path="/sbin/ifconfig" dev=dm-0 ino=44
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:ifconfig_exec_t:s0 tclass=file
type=AVC msg=audit(1373816913.953:22): avc:  denied  { read } for  pid=1416
comm="ifconfig" name="unix" dev=proc ino=4026532007
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:proc_net_t:s0 tclass=file
type=AVC msg=audit(1373816913.954:23): avc:  denied  { search } for
 pid=1416 comm="ifconfig" scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:sysctl_net_t:s0 tclass=dir
type=AVC msg=audit(1373816913.954:24): avc:  denied  { open } for  pid=1416
comm="ifconfig" name="dev" dev=proc ino=4026531979
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:proc_net_t:s0 tclass=file
type=AVC msg=audit(1373816913.954:25): avc:  denied  { getattr } for
```

```
 pid=1416 comm="ifconfig" path="/proc/1416/net/dev" dev=proc ino=4026531979
scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:proc_net_t:s0 tclass=file
type=AVC msg=audit(1373816914.351:26): avc:  denied  { sys_tty_config } for
 pid=1423 comm="rm" capability=26
 scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:system_r:passenger_t:s0 tclass=capability
type=AVC msg=audit(1373816974.509:44): avc:  denied  { getattr } for
 pid=1303 comm="ruby"
path="/opt/rh/ruby193/root/usr/var/lib/puppet/.puppet/ssl/certs/foreman.xiolab.lab.abc.com.pem"
dev=dm-0 ino=792301 scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:var_lib_t:s0 tclass=file
type=AVC msg=audit(1373817034.643:45): avc:  denied  { name_bind } for
 pid=1303 comm="ruby" src=17117 scontext=system_u:system_r:passenger_t:s0
tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
```

Second bunch reported by me running nightly (occurs after some time even when Foreman is not accessed at all):

1. grep AVC /var/log/audit/audit.log | paste
   http://sprunge.us/SgXE

1. cat /var/log/audit/audit.log | audit2allow -R | paste
   http://sprunge.us/HQDf

Associated revisions

Revision 36c7bfaa - 07/24/2013 10:14 AM - Lukas Zapletal

fixes #2789 - selinux denials, httpd_tmp_t, rlimits, postgresql sockets

Revision ba3378a8 - 07/24/2013 10:15 AM - Lukas Zapletal

fixes #2789 - selinux denials, httpd_tmp_t, rlimits, postgresql sockets

(cherry picked from commit 36c7bfaa763fd403c78f2419d51198473e3ce2f6)

History

#1 - 07/17/2013 08:57 AM - Dominic Cleal

- Project changed from Foreman to SELinux

- Category deleted (56)

#2 - 07/22/2013 08:40 AM - Dominic Cleal

- Status changed from New to Ready For Testing

https://github.com/theforeman/foreman-selinux/pull/4

#3 - 07/24/2013 04:42 PM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset ba3378a8671b1d88ec1b865f2942050ec993e395.

#4 - 07/11/2018 03:33 PM - Anonymous

- Target version deleted (1.2.1)