SELinux - Bug #5910

Puppet or puppetmaster sometimes changes file contexts

05/23/2014 01:11 PM - Lukas Zapletal

Status:	Closed		
Priority:	Normal		
Assignee:	Lukas Zapletal		
Category:	Packaging		
Target version:	1.5.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1107673	**Red Hat JIRA:**	
Pull request:			

Description

which is prevented by SELinux. This has something to do with selinux users and RHEL6. Discussion is here:

```
14:56    lzap | dwalsh: https://gist.github.com/lzap/b2c29cd20da2a0d95459
14:57    lzap | dwalsh: mirek told me the other day I see relabelto because the process is touchin
g xattrs most likely. whatever, I'd like to allow that, but
             | my rules do not apply for some reason
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
14:58  dwalsh | lzap, You are relabeling a file to system_u:...  You are running as unconfined_u.
 THere is a constraint that says you are not allowed to do
             | this unless you have a certain attribute.
14:58  dwalsh | scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_lo
g_t:s0
14:58  dwalsh | Is passenger_t doing a setfilecon?
15:00  dwalsh | lzap, It looks like you ran passenger from an unconfined_u user,
15:00    lzap | oh
15:00    lzap | like started it from shell right?
15:01  dwalsh | lzap, I would not have a problem doing it.  We really do not enforce on user part
of the label.
15:01  dwalsh | Did you do a runcon to get the service to start?
15:01    lzap | it was puppet who started that
15:01    lzap | puppet agent
15:01    lzap | but puppet stareted from openstack installer
15:01    lzap | and that was obviously started as root
15:02    lzap | but I'd expect when I'd do service start it would start normally
15:02    lzap | puppet is doing: service httpd start
15:02  dwalsh | is this RHEL6?
15:02    lzap | yes
15:02    lzap | 6.54
15:02    lzap | 6.5
15:03  dwalsh | Well puppet must have been running as unconfined_u which means someone restarted i
t.
15:03  dwalsh | In RHEL7 this would not be a problem because services would be started via systemd
, which would be running as system_u.
15:04  dwalsh | domain_subj_id_change_exemption(passenger_t) would fix the problem.
15:04  dwalsh | Most of the time passenger_t would run as system_u, since it would be started at b
oot time.  But if a user did a service restart, then I guess
             | this could happen.
15:05    lzap | so you are telling me that all services which are running under RHEL6 and are conf
ined can go wrong as soon as root restarts them from a shell?
15:06  dwalsh | No only services that attempt to do built in SELinux calls.
15:06  dwalsh | Puppet must be doing a setfiles() call to change the label.
15:07    lzap | ok I will investigate this, but I'd not expect this there
15:07    lzap | it's a ruby app without any selinux support
15:07    lzap | I mean the upstream code
15:07    lzap | and I am not aware of any special handling in our startup scripts or something
```

```
15:08  dwalsh | We added selinux support to ruby a few years ago to be used with puppet.
15:08  dwalsh | Search the code for matchpathcon, and setfilecon.
```

Associated revisions

Revision a39d8de2 - 05/30/2014 09:37 AM - Lukas Zapletal

Fixes #5910 - Puppetmaster allowed to set file contexts

History

#1 - 05/23/2014 01:14 PM - Lukas Zapletal

```
# audit2allow -aRl

require {
    type passenger_t;
    type puppet_log_t;
    type foreman_lib_t;
    type puppet_var_lib_t;
    class lnk_file read;
    class dir relabelto;
    class file relabelto;
}

#============= passenger_t ==============
allow passenger_t foreman_lib_t:lnk_file read;

#!!!! This avc is a constraint violation.  You will need to add an attribute to either the source or target ty
pe to make it work.
#Contraint rule:
allow passenger_t puppet_log_t:file relabelto;

#!!!! This avc is a constraint violation.  You will need to add an attribute to either the source or target ty
pe to make it work.
#Contraint rule:
allow passenger_t puppet_var_lib_t:dir relabelto;

#!!!! This avc is a constraint violation.  You will need to add an attribute to either the source or target ty
pe to make it work.
#Contraint rule:
allow passenger_t puppet_var_lib_t:file relabelto;
```

#2 - 05/26/2014 11:26 AM - Lukas Zapletal

- Category set to Packaging

- Status changed from New to Ready For Testing

- Target version set to 1.8.2

Solved with great help of Mirek Grepl, thanks.

https://github.com/theforeman/foreman-selinux/pull/18

#3 - 05/28/2014 10:07 AM - Dominic Cleal

- translation missing: en.field_release set to 16

#4 - 05/30/2014 10:47 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset a39d8de2e0ab1f042acb21e446773d7d8496d25e.

#5 - 06/10/2014 12:46 PM - Bryan Kearney

- Bugzilla link set to https://bugzilla.redhat.com/show_bug.cgi?id=1107673