

Installer - Bug #5924

Puppetmaster denial for node.rb

05/26/2014 10:50 AM - Lukas Zapletal

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	
I am getting this one:	
type=AVC msg=audit(1401094926.717:390): avc: denied { execute } for pid=15328 comm="ruby" name="node.rb" dev=dm-0 ino=2102058 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file	
type=AVC msg=audit(1401094926.717:390): avc: denied { execute_no_trans } for pid=15328 comm="ruby" path="/etc/puppet/node.rb" dev=dm-0 ino=2102058 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file	
I think I saw that previously.	
Related issues:	
Related to SELinux - Bug #3895: AVC denials from Foreman 1.3 installation	Resolved 12/17/2013

History

#1 - 05/26/2014 10:51 AM - Lukas Zapletal

- Related to Bug #3895: AVC denials from Foreman 1.3 installation added

#2 - 05/26/2014 10:52 AM - Lukas Zapletal

Ok it looks like this was not resolved (see the related bug). We need a rule for this.

#3 - 05/26/2014 11:13 AM - Lukas Zapletal

- Category set to Packaging

- Status changed from New to Ready For Testing

- Assignee set to Lukas Zapletal

- Target version set to 1.8.2

Ok the problem appears when node.rb has puppet_etc_t. After we call foreman-selinux-relabel the context is corrected. It looks like we deploy node.rb via puppet, therefore the relabel step is called BEFORE (during foreman-selinux rpm transaction). Thus it has wrong context.

```
[root@ibm-hs23-02 ~]# foreman-selinux-relabel
/sbin/restorecon reset /usr/share/foreman/config/hooks context system_u:object_r:bin_t:s0->system_u:object_r:foreman_hook_t:s0
/sbin/restorecon reset /etc/foreman context system_u:object_r:etc_t:s0->system_u:object_r:foreman_config_t:s0
/sbin/restorecon reset /etc/foreman/client_key.pem context system_u:object_r:etc_t:s0->system_u:object_r:foreman_config_t:s0
/sbin/restorecon reset /etc/foreman/encryption_key.rb context unconfined_u:object_r:etc_t:s0->unconfined_u:object_r:foreman_config_t:s0
/sbin/restorecon reset /etc/foreman/client_ca.pem context unconfined_u:object_r:etc_t:s0->unconfined_u:object_r:foreman_config_t:s0
/sbin/restorecon reset /etc/foreman/database.yml context system_u:object_r:etc_t:s0->system_u:object_r:foreman_config_t:s0
/sbin/restorecon reset /etc/foreman/client_cert.pem context unconfined_u:object_r:etc_t:s0->unconfined_u:object_r:foreman_config_t:s0
/sbin/restorecon reset /etc/foreman/settings.yml context system_u:object_r:etc_t:s0->system_u:object_r:foreman_config_t:s0
```

```
/sbin/restorecon reset /etc/foreman/email.yaml context system_u:object_r:etc_t:s0->system_u:object_r:foreman_conf_t:s0
/sbin/restorecon reset /etc/foreman/plugins context system_u:object_r:etc_t:s0->system_u:object_r:foreman_conf_t:s0
/sbin/restorecon reset /etc/foreman/plugins/katello.yaml context system_u:object_r:etc_t:s0->system_u:object_r:foreman_conf_t:s0
/sbin/restorecon reset /etc/foreman/plugins/katello context system_u:object_r:etc_t:s0->system_u:object_r:foreman_conf_t:s0
/sbin/restorecon reset /etc/foreman/plugins/katello/client.conf context system_u:object_r:etc_t:s0->system_u:object_r:foreman_conf_t:s0
/sbin/restorecon reset /etc/puppet/node.rb context system_u:object_r:puppet_etc_t:s0->system_u:object_r:foreman_etc_t:s0
```

Ignore all the lines except the node.rb - this is bug in RHEL6 which will likely never be fixed: if a context is an alias, then restorecon restores to original context rather than alias.

Rather than relabeling this, I have decided to drop foreman_etc_t and use puppet_etc_t instead. It is not big deal since there are none dangerous executable files with this domain.

Putting the fix into: <https://github.com/theforeman/foreman-selinux/pull/18>

#4 - 05/29/2014 11:05 AM - Lukas Zapletal

- Project changed from SELinux to Installer
- Category deleted (Packaging)

Instead of dropping the type, I will make sure that installer sets proper selinux file label.

#5 - 06/11/2014 02:53 PM - Anonymous

- Target version changed from 1.8.2 to 1.8.1

#6 - 06/18/2014 01:27 PM - Lukas Zapletal

- Status changed from Ready For Testing to Assigned

This issue was NOT fixed in the PR mentioned. I need to do seltype in Puppet.

#7 - 06/26/2014 03:17 PM - Lukas Zapletal

- Status changed from Assigned to Ready For Testing

<https://github.com/theforeman/puppet-foreman/pull/197>

#8 - 07/07/2014 07:22 AM - Anonymous

- Target version changed from 1.8.1 to 1.8.0

#9 - 07/07/2014 09:46 AM - Dominic Cleal

Seen on a second run of the installer:

```
# [ WARN 2014-07-07 14:37:02 verbose] /File[/etc/puppet/node.rb]/seltype: seltype changed 'puppet_etc_t' to 'foreman_etc_t'
```

This agrees with the theory presented in the PR comments, which is that it's ordering related (node.rb being evaled before foreman-selinux is installed).

#10 - 07/30/2014 06:49 AM - Anonymous

- Target version changed from 1.8.0 to 1.7.5

#11 - 08/04/2014 09:39 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100
- translation missing: en.field_release set to 10

<https://github.com/theforeman/foreman-packaging/commit/068b03a618679c8a2c6b5309351c51ac60e7cab7>