# SELinux - Feature #4113

## Restrict Foreman not to be able to write to /usr/share/foreman

01/17/2014 08:12 AM - Lukas Zapletal

| | | | |
|---|---|---|---|
| **Status:** | New | | |
| **Priority:** | Low | | |
| **Assignee:** | Lukas Zapletal | | |
| **Category:** | | | |
| **Target version:** | | | |
| **Difficulty:** | | **Fixed in Releases:** | |
| **Triaged:** | | **Found in Releases:** | |
| **Bugzilla link:** | | **Red Hat JIRA:** | |
| **Pull request:** | | | |

**Description**

Currently Foreman is allowed to write to foreman_lib_t:

```
read_files_pattern(httpd_t, foreman_lib_t, foreman_lib_t)
    manage_files_pattern(passenger_t, foreman_lib_t, foreman_lib_t)
    manage_dirs_pattern(passenger_t, foreman_lib_t, foreman_lib_t)
```

We should tighten this and also make sure that public/avatar directory is in different domain (writable).

## History

**#1 - 01/17/2014 08:15 AM - Lukas Zapletal**

Also, we are not explicitly setting file contexts for /usr/share/foreman in foreman.fc. We should do that, users are not able to fix file policies.

And this line is twice:

```
manage_dirs_pattern(httpd_foreman_script_t, foreman_lib_t , foreman_lib_t)
manage_dirs_pattern(httpd_foreman_script_t, foreman_lib_t , foreman_lib_t)
```

**#2 - 03/03/2014 01:25 PM - Anonymous**

*- Target version set to 1.9.0*

**#3 - 03/26/2014 01:33 PM - Anonymous**

*- Target version changed from 1.9.0 to 1.8.4*

**#4 - 04/24/2014 12:09 PM - Lukas Zapletal**

*- Status changed from New to Assigned*

*- Assignee set to Lukas Zapletal*

**#5 - 04/24/2014 12:13 PM - Anonymous**

*- Target version changed from 1.8.4 to 1.8.3*

**#6 - 04/25/2014 10:20 AM - Lukas Zapletal**

I will implement this change POST 1.5 release, because this refactoring can bring some issues.

**#7 - 05/21/2014 01:21 PM - Anonymous**

*- Target version deleted (1.8.3)*

**#8 - 07/30/2014 04:41 AM - Ohad Levy**

*- translation missing: en.field_release set to 10*

**#9 - 07/30/2014 09:13 AM - Lukas Zapletal**

*- Status changed from Assigned to New*

*- Priority changed from Normal to Low*

*- translation missing: en.field_release deleted (10)*