SELinux - Feature #26520
Allow execmem for passenger due to Ruby FFI
04/03/2019 09:47 AM - Lukas Zapletal

Status: Closed
Priority: Normal
Assignee: Lukas Zapletal
Category: General Foreman
Target version: 1.22.0
Difficulty: 

Pull request: https://github.com/Katello/katello-selinux/pull/19

Fixed in Releases: 1.22.0
Found in Releases: 

Description
Ruby library ethon which is used by Katello (katello - zest - typhoeus - ethon - ffi) uses FFI to load a libcurl. This was previously not required and Foreman core only used FFI in the asset compilation which is not being executed in runtime. With new Katello Pulp v3API this is now a runtime library, however SELinux prevents FFI from operation due to memory execution:

```ruby
Error ID: 003a694f
Message from application: (RuntimeError)
/opt/theforeman/tfm/root/usr/share/gems/gems/ffi-1.4.0/lib/ffi/library.rb:253:in `attach
/opt/theforeman/tfm/root/usr/share/gems/gems/ffi-1.4.0/lib/ffi/library.rb:253:in `attach_function'
/opt/theforeman/tfm/root/usr/share/gems/ethon-0.12.0/lib/ethon/libc.rb:16:in `<module:Libc>
/of```
The missing rule is:

```
allow passenger_t self:process execmem;
```

We are tracking the same problem for Smart Proxy (OpenSCAP plugin), the same reason: FFI.

Now, further investigation shows that FFI authors do not think this is a problem, they did not find a workaround in the FFI code as a good option and they recommend to allow this in SELinux in the official documentation:

- https://bitbucket.org/cffi/cffi/issues/231

We are going to allow this rule for both Foreman (passenger) and Smart proxy as there is no easy workaround anyway.

---

**Related issues:**

<table>
<thead>
<tr>
<th>Related to SELinux - Bug #16273: SELinux Preventing Foreman Proxy From Starting</th>
<th>Closed</th>
</tr>
</thead>
</table>

---

**History**

**#1 - 04/03/2019 09:47 AM - Lukas Zapletal**
- Category set to General Foreman
- Project changed from Foreman to SELinux

**#2 - 04/03/2019 09:49 AM - Lukas Zapletal**
- Related to Bug #16273: SELinux Preventing Foreman Proxy From Starting added

**#3 - 04/03/2019 09:53 AM - The Foreman Bot**
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman-selinux/pull/88 added

**#4 - 04/03/2019 10:27 AM - Tomer Brisker**
- Target version set to 1.22.0

**#5 - 04/24/2019 12:30 PM - Tomer Brisker**
- Status changed from Ready For Testing to Closed
- Fixed in Releases 1.22.0 added
- Pull request https://github.com/Katello/katello-selinux/pull/19 added
- Pull request deleted (https://github.com/theforeman/foreman-selinux/pull/88)