SELinux - Bug #5827

katello-installer generates AVC: denied { name_connect } for scontext=passenger_t:s0 tcontext=:websm_port_t:s0 tclass=tcp_socket

05/20/2014 03:20 PM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Lukas Zapletal		
Category:	Packaging		
Target version:	1.6.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1078265	**Red Hat JIRA:**	
Pull request:			

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1078265
Description of problem:
katello-installer generates AVCs

Version-Release number of selected component (if applicable):
Satellite-6.0.3-RHEL-6-20140318.3

How reproducible:
always

Steps to Reproduce:
1. # katello-installer
2. # katello-installer --capsule-parent-fqdn <fqdn> --capsule-dns true --capsule-dns-forwarders 10.16.36.29 --capsule-dns-forwarders 10.11.5.19 --capsule-dns-forwarders 10.5.30.160 --capsule-dns-interface eth0 --capsule-dns-zone katellolabs.org --capsule-dhcp true --capsule-dhcp-interface eth0 --capsule-tftp true --capsule-puppet true --capsule-puppetca true --capsule-register-in-foreman true --capsule-foreman-oauth-secret <secret> --capsule-pulp false

Actual results: === katello-installer ===
SELinux: 2048 avtab hash slots, 278892 rules.
SELinux: 2048 avtab hash slots, 278892 rules.
SELinux: 9 users, 12 roles, 3937 types, 220 bools, 1 sens, 1024 cats
SELinux: 81 classes, 278892 rules

=== katello-installer --capsule-parent-fqdn <fqdn> --capsule-dns true --capsule-dns-forwarders 10.16.36.29 --capsule-dns-forwarders 10.11.5.19 --capsule-dns-forwarders 10.5.30.160 --capsule-dns-interface eth0 --capsule-dns-zone katellolabs.org --capsule-dhcp true --capsule-dhcp-interface eth0 --capsule-tftp true --capsule-puppet true --capsule-puppetca true --capsule-register-in-foreman true --capsule-foreman-oauth-secret <secret> --capsule-pulp false ===
time->Sun Mar 16 17:17:03 2014
type=SYSCALL msg=audit(1395004623.756:191): arch=c000003e syscall=42 success=no exit=-111 a0=f a1=7f5cc05faf00 a2=1c a3=ff00 items=0 ppid=23315 pid=23863 auid=4294967295 uid=497 gid=497 euid=497 suid=497 fsuid=497 egid=497 sgid=497 fsgid=497 tty=(none) ses=4294967295 comm="ruby" exe="/opt/rh/ruby193/root/usr/bin/ruby"
subj=unconfined_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1395004623.756:191): avc: denied { name_connect } for pid=23863 comm="ruby" dest=9090 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:websm_port_t:s0 tclass=tcp_socket
Fail: AVC messages found.

Expected results:
No AVCs should be generated

Additional info:
This is most probably a known issue, but filling it as I have not seen it anywhere.

Associated revisions

Revision b13ec514 - 05/30/2014 09:42 AM - Lukas Zapletal

History

#1 - 05/20/2014 03:22 PM - Dominic Cleal

The issue looks to be that katello-installer has moved the smart proxy port from 8443 to 9090, so the default policy doesn't work.

By default passenger_t is permitted name_connect to http_port_t which contains 8443. I'd suggest two changes:

- add a new port type for the smart proxy that passenger_t is permitted to connect to, include 8443/tcp by default
- have the foreman_proxy installer module add the $port to this SELinux port range

#2 - 05/23/2014 11:37 AM - Lukas Zapletal

- Category set to Packaging

- Status changed from New to Assigned

- Assignee set to Lukas Zapletal

- Target version set to 1.8.2

#3 - 05/26/2014 01:38 PM - Lukas Zapletal

That sounds like a decent plan, but unfortunately port 9090 is already taken by websm service (no clue what this is). Since it is a very bad practice to redefine existing ports, I am adding 9090 into the core policy as hardcoded value (websm_port_t). But in addition to that, new port context foreman_proxy_port_t was defined so any port number can be added by users.

This has been documented here: http://projects.theforeman.org/projects/foreman/wiki/SELinux

#4 - 05/26/2014 01:42 PM - Lukas Zapletal

- Status changed from Assigned to Ready For Testing

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

#5 - 05/28/2014 10:07 AM - Dominic Cleal

- translation missing: en.field_release set to 10

#6 - 05/30/2014 10:47 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset b13ec514c1616dcea4ba90f3c6794827d9957db5.