

Summary:

SELinux is preventing restorecon (setfiles_t) "read" unconfined_notrans_t.

Detailed Description:

SELinux denied access requested by restorecon. It is not expected that this access is required by restorecon and this access may signal an intrusion attempt. It is also possible that the specific version or configuration of the application is causing it to require additional access.

Allowing Access:

You can generate a local policy module to allow this access - see FAQ (<http://fedora.redhat.com/docs/selinux-faq-fc5/#id2961385>) Or you can disable SELinux protection altogether. Disabling SELinux protection is not recommended. Please file a bug report (http://bugzilla.redhat.com/bugzilla/enter_bug.cgi) against this package.

Additional Information:

Source Context	unconfined_u:system_r:setfiles_t:s0-s0:c0.c1023
Target Context	unconfined_u:system_r:unconfined_notrans_t:s0-s0:c0.c1023
Target Objects	pipe [fifo_file]
Source	restorecon
Source Path	/sbin/setfiles
Port	<Unknown>
Host	localhost.localdomain
Source RPM Packages	policycoreutils-2.0.52-8.fc9
Target RPM Packages	
Policy RPM	selinux-policy-3.3.1-107.fc9
Selinux Enabled	True
Policy Type	targeted
MLS Enabled	True
Enforcing Mode	Enforcing
Plugin Name	catchall
Host Name	localhost.localdomain
Platform	Linux localhost.localdomain 2.6.27.5-41.fc9.i686 #1 SMP Thu Nov 13 20:52:14 EST 2008 i686 i686
Alert Count	2
First Seen	Sun 14 Dec 2008 01:31:38 AM KST
Last Seen	Sun 14 Dec 2008 01:31:42 AM KST
Local ID	added84b-78f7-490a-b72d-489bf9ccbcc7
Line Numbers	

Raw Audit Messages

```
node=localhost.localdomain type=AVC msg=audit(1229185902.633:1237): avc: denied { read } for pid
node=localhost.localdomain type=SYSCALL msg=audit(1229185902.633:1237): arch=40000003 syscall=11 su
```