Packages - Packaging Request #1516

[auditd-openrc] add to PCR

2017-11-03 08:34 AM - ToffeeYogurtPots

Status:	open	**% Done:**	0%
Priority:	wish		
Assignee:			
Category:			

Description

I'm having an issue with AppArmor and it's logs. Users on #apparmor (OFTC not freenode) recommended using auditd. However there is no auditd-openrc package currently and rsyslog-openrc doesn't appear to work either (no APPROVED or DENIED messages appear in /var/log). The Hyperbola devs are also looking for this: https://issues.hyperbola.info/index.php?do=details&task_id=4 .

Steps to reproduce:

1. Install OpenRC.
2. Setup AppArmor (install compatible kernel, apparmor-openrc etc).
3. Install rsyslog-openrc.
4. Run "rc-service rsyslog start".
5. Run "aa-genprof iceweasel" (it can be any program, even CLI stuff).
6. Leave aa-genprof running and close any instances of the program you chose and then open it again.
7. Now go back to the aa-genprof terminal and press "S" for scan. The expected outcome is that it should scan /var/log and find all of the "APPROVED" lines and prompt you as to whether they should be allowed or denied. However, the current outcome is that it loops back asking "[(S)can system log for AppArmor events] / (F)inish" again since it finds nothing in /var/log.
8. Run "grep -r apparmor= /var/log", the expected outcome should be a lot of "APPROVED" or "DENIED" messages but in my case there are none.

Possible Solution(s):

- Add auditd-openrc package and hope that it resolves the issue
  Description: Auditd init script for OpenRC
  License: GPLv2
  AUR: https://aur.archlinux.org/packages/auditd-openrc/ (completely broken, sha256sums outdated and sed lines don't work)
  Init Script: https://gitweb.gentoo.org/repo/gentoo.git/plain/sys-process/audit/files/auditd-init.d-2.4.3