

4.2.1.3 Ensure rsyslog default file permissions configured (Scored)

Profile Applicability

```
Level 1 - Server  
Level 1 - Workstation
```

Description

rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit

Run the following command and verify that `$FileCreateMode` is `0640` or more restrictive:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf
```

Remediation

Edit the `/etc/rsyslog.conf` and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

References

See the `rsyslog.conf(5)` man page for more information.

Notes

You should also ensure this is not overridden with less restrictive settings in any `/etc/rsyslog.d/*` conf file.

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/centos7/4/2/1/3>

Last update: **2017/05/04 17:19**

