

1.1.3 Ensure nodev option set on /tmp partition (Scored)

Profile Applicability

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

Description

The nodev mount option specifies that the filesystem cannot contain special devices.

Rationale

Since the /tmp filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in /tmp.

Audit

If a /tmp partition exists run the following command and verify that the nodev option is set on /tmp:

```
# mount | grep /tmp  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to add nodev to the /tmp mount options:

```
[Mount]  
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount /tmp:

```
[Mount]  
# mount -o remount,nodev /tmp
```

Notes

systemd includes the tmp.mount service which should be used instead of configuring /etc/fstab. Mounting options are configured in the Options setting in /etc/systemd/system/tmp.mount.

From:

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

Permanent link:

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

Last update: **2017/05/05 16:40**

