

# 1.1.4 Ensure nosuid option set on /tmp partition (Scored)

## Profile Applicability

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

## Description

The nosuid mount option specifies that the filesystem cannot contain setuid files.

## Rationale

Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp.

## Audit

If a /tmp partition exists run the following command and verify that the nosuid 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 nosuid to the /tmp mount options:

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

Run the following command to remount /tmp:

```
# mount -o remount,nosuid /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/centos7/1/1/4>

Last update: **2017/05/05 17:29**

