

1.1.16 Ensure nosuid option set on /dev/shm partition (Scored)

Profile Applicability

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

Description

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

Rationale

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit

Run the following command and verify that the nosuid option is set on /dev/shm.

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

Remediation

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information. Run the following command to remount /dev/shm:

```
# mount -o remount,nosuid /dev/shm
```

Notes

/dev/shm is not specified in /etc/fstab despite being mounted by default. The following line will implement the recommended /dev/shm mount options in /etc/fstab:

```
tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

From:

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

Permanent link:

<https://secscan.acron.pl/centos7/1/1/16>

Last update: **2017/05/05 20:17**

