1.1.7 Ensure separate partition exists for /var/tmp (Scored)

Profile Applicability

```
Level 2 - Server
Level 2 - Workstation
```

Description

The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale

Since the `/var/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/var/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/var/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Audit

Run the following command and verify output shows `/var/tmp` is mounted:

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

Remediation

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/tmp`. For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.