1.1.21 Disable Automounting (Scored)

Profile Applicability

```
Level 1 - Server
Level 2 - Workstation
```

Description

`autofs` allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Audit

Run the following command to verify `autofs` is not enabled:

```
# systemctl is-enabled autofs
disabled
```

Verify result is not “enabled”.

Remediation

Run the following command to disable `autofs`:

```
# systemctl disable autofs
```

Impact

The use portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Notes

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.