6.2.10 Ensure users' dot files are not group or world writable (Scored)

Profile Applicability

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

Description

While the system administrator can establish secure permissions for users' “dot” files, the users can easily override these.

Rationale

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit

Run the following script and verify no results are returned:

```
#!/bin/bash
for dir in `cat /etc/passwd | egrep -v '(root|sync|halt|shutdown)' | awk -F:
'($7 != "/usr/sbin/nologin") { print $6 }'`; do
  for file in $dir/.[A-Za-z0-9]*; do
    if [ ! -h "$file" -a -f "$file" ]; then
      fileperm=`ls -ld $file | cut -f1 -d" "`
      if [ `echo $fileperm | cut -c6 ` != "-" ]; then
       echo "Group Write permission set on file $file"
      fi
      if [ `echo $fileperm | cut -c9 ` != "-" ]; then
       echo "Other Write permission set on file $file"
      fi
    fi
  done
done
```

Remediation

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.