6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Scored)

Profile Applicability

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

Description

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale

Group or world-writable user home directories 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|halt|sync|shutdown)' | awk -F:
'($7 != "/usr/sbin/nologin") { print $6 }'`; do
  dirperm=`ls -ld $dir | cut -f1 -d" "`
  if [ `echo $dirperm | cut -c6 ` != "-" ]; then
    echo "Group Write permission set on directory $dir"
  fi
  if [ `echo $dirperm | cut -c8 ` != "-" ]; then
    echo "Other Read permission set on directory $dir"
  fi
  if [ `echo $dirperm | cut -c9 ` != "-" ]; then
    echo "Other Write permission set on directory $dir"
  fi
  if [ `echo $dirperm | cut -c10 ` != "-" ]; then
    echo "Other Execute permission set on directory $dir"
  fi
```

done

Remediation

Making global modifications to user home directories 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 file permissions and determine the action to be taken in accordance with site policy.