6.2.6 Ensure root PATH Integrity (Scored)

Profile Applicability

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

Description

The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.

Rationale

Including the current working directory (.) or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

Audit

Run the following script and verify no results are returned:

```
#!/bin/bash
if [ "`echo $PATH | grep :: `" != "" ]; then
  echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | grep :$`" != "" ]; then
  echo "Trailing : in PATH"
fi
p=`echo $PATH | sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
  if [ "$1" = "." ]; then
    echo "PATH contains ."
    shift
    continue
  fi
  if [ -d $1 ]; then
    dirperm=`ls -ldH $1 | cut -f1 -d" "`
    if [ `echo $dirperm | cut -c6 ` != "-" ]; then
      echo "Group Write permission set on directory $1"
```

```
    fi
  if [ `echo $dirperm | cut -c9 ` != "-" ]; then
    echo "Other Write permission set on directory $1"
  fi
  dirown=`ls -ldH $1 | awk '{print $3}'`
  if [ "$dirown" != "root" ] ; then
    echo $1 is not owned by root
  fi
  else
    echo $1 is not a directory
  fi
  shift
done
```

Remediation

Correct or justify any items discovered in the Audit step.