

6.2.17 Ensure no duplicate GIDs exist (Scored)

Profile Applicability

Level 1 - Server
Level 1 - Workstation

Description

Although the groupadd program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the /etc/group file and change the GID field.

Rationale

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit

Run the following script and verify no results are returned:

```
#!/bin/bash
cat /etc/group | cut -f3 -d":" | sort -n | uniq -c | while read x ; do
  [ -z "${x}" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    groups=`awk -F: '($3 == n) { print $1 }' n=$2 /etc/group | xargs`
    echo "Duplicate GID ($2): ${groups}"
  fi
done
```

Remediation

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Notes

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/centos7/6/2/17>

Last update: **2017/05/04 19:06**

