

6.1.13 Audit SUID executables (Not Scored)

Profile Applicability

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

Description

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges..

Rationale

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit

Run the following command to list SUID files:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -  
xdev -type f -perm -4000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

Remediation

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

From:

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

Permanent link:

<https://secscan.acron.pl/centos7/6/1/13>

Last update: **2017/05/04 19:00**

