

6.1.10 Ensure no world writable files exist (Scored)

Profile Applicability

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

Description

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit

Run the following command and verify no files are returned:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -  
xdev -type f -perm -0002
```

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 -0002
```

Remediation

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given

file.

From:

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

Permanent link:

<https://secscan.acron.pl/ubuntu1604/6/1/10>

Last update: **2017/05/04 13:08**

