

6.2.4 Ensure no legacy "+" entries exist in /etc/group (Scored)

Profile Applicability

Level 1 - Server
Level 1 - Workstation

Description

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit

Run the following command and verify that no output is returned:

```
# grep '^+: ' /etc/group
```

Remediation

Remove any legacy '+' entries from /etc/group if they exist.

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

Permanent link:
<https://secscan.acron.pl/centos7/6/2/4>

Last update: **2017/05/04 19:02**

