Gentoo Linux Frequently Forgotten Changes

XCCDF Security Guide

Gentoo Linux Frequently Forgotten Changes: XCCDF Security Guide

Generated by OpenSCAP (1.0.2) on 2013-12-16T11:16:06+01:00.

Table of Contents

List of Figures

Chapter 1. Installation related settings

In this chapter, we will cover the installation related settings users forget to enable or change.

Change the /dev/ROOT and /dev/BOOT entries in /etc/fstab

During the installation, Gentoo provides a default /etc/fstab file which contains substitution names like /dev/ROOT and /dev/BOOT.

Users should change these towards the right block device that represents their root and boot file systems. However, many users forget this. If the /dev/ROOT is not changed, most systems will still boot (as it is the Linux kernel and its options that define what the root file system is) but automated checks or other system updates might show undefined behavior if this is not correctly changed.

The /dev/BOOT change is needed for the bootloader (and sometimes also kernel deployment) changes. The processes could try to mount /dev/BOOT, which will fail, terminating the process and showing an ugly error message to the end user.

There should be no /dev/ROOT in /etc/fstab

Figure 1.1. There should be no /dev/ROOT in /etc/fstab – remediation instructions

Update /etc/fstab and change /dev/ROOT to point to the right block device containing the root file system.

There should be no /dev/BOOT in /etc/fstab

Figure 1.2. There should be no /dev/BOOT in /etc/fstab – remediation instructions

Update /etc/fstab and change /dev/BOOT to point to the right block device containing the boot file system.

Define rc_sys in rc.conf

The rc_sys variable in rc.conf tells OpenRC which kind of hypervisor, if any, the system is installed in. It should be set to the correct value, or empty if there is no hypervisor involved.

Keeping this variable unset will continuously show a warning, and OpenRC will assume no virtualization is enabled.

rc_sys should be defined in /etc/rc.conf

Figure 1.3. rc_sys should be defined in /etc/rc.conf – remediation instructions

Update /etc/rc.conf's rc_sys variable to the right value.

Figure 1.4. rc_sys should be defined in /etc/rc.conf – remediation script

```
sed -i 's/^#rc_sys.*/rc_sys="" # Auto-remediated/g' /etc/rc.conf;
```

Chapter 2. Rule Selection

Based on profile: **With remediation** (xccdf_org.gentoo.dev.swift_profile_remediation)

This profile contains all the checks that have remediation.