# OpenSCAP Evaluation Report

# Guide to the Secure Configuration of Red Hat Enterprise Linux 7

with profile United States Government Configuration Baseline

— This compliance profile reflects the core set of security related configuration settings for deployment of Red Hat Enterprise Linux 7.x into U.S. Defense, Intelligence, and Civilian agencies. Development partners and sponsors include the U.S. National Institute of Standards and Technology (NIST), U.S. Department of Defense, the National Security Agency, and Red Hat.

This baseline implements configuration requirements from the following sources:

- Committee on National Security Systems Instruction No. 1253 (CNSSI 1253)
- NIST Controlled Unclassified Information (NIST 800-171)
- NIST 800-53 control selections for MODERATE impact systems (NIST 800-53)
- U.S. Government Configuration Baseline (USGCB)
- NIAP Protection Profile for General Purpose Operating Systems v4.0 (OSPP v4.0)
- DISA Operating System Security Requirements Guide (OS SRG)

For any differing configuration requirements, e.g. password lengths, the stricter security setting was chosen. Security Requirement Traceability Guides (RTMs) and sample System Security Configuration Guides are provided via the scap-security-guide-docs package.

This profile reflects U.S. Government consensus content and is developed through the OpenSCAP/SCAP Security Guide initiative, championed by the National Security Agency. Except for differences in formatting to accommodate publishing processes, this profile mirrors OpenSCAP/SCAP Security Guide content as minor divergences, such as bugfixes, work through the consensus and release processes.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG for Red Hat Enterprise Linux 7, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

# Evaluation Characteristics

| | |
|---|---|
| **Evaluation target** | bastion.pichuang.local |
| **Benchmark URL** | ./ssg-rhel7-ds.xml |
| **Benchmark ID** | xccdf_org.ssgproject.content_benchmark_RHEL-7 |
| **Profile ID** | xccdf_org.ssgproject.content_profile_ospp |
| **Started at** | 2019-06-23T21:31:51 |
| **Finished at** | 2019-06-23T21:36:04 |
| **Performed by** | pichuang |

### CPE Platforms

- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client
- cpe:/o:redhat:enterprise_linux:7::computenode

### Addresses

- IPv4 127.0.0.1
- IPv4 192.168.77.9
- IPv4 172.17.0.1
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:d92b:e6ad:a5e9:42bd
- IPv6 fe80:0:0:0:42:b4ff:fed6:e7fc
- IPv6 fe80:0:0:0:301b:e1ff:fe5d:e2af
- MAC 00:00:00:00:00:00
- MAC 8C:16:45:67:32:02
- MAC 02:42:B4:D6:E7:FC
- MAC 32:1B:E1:5D:E2:AF

# Compliance and Scoring

**The target system did not satisfy the conditions of 197 rules!** Furthermore, the results of 21 rules were inconclusive. Please review rule results and consider applying remediation.

## Rule results


## Severity of failed rules


## Score

| Scoring system | Score | Maximum | Percent |
|---|---|---|---|
| urn:xccdf:scoring:default | 60.074036 | 100.000000 | 60.07% |

# Rule Overview

- [x] pass
- [x] fixed
- [x] informational
- [x] fail
- [x] error
- [x] unknown

unknown

notchecked

notapplicable

Search through XCCDF rules | Search

Group rules by: Default

| Title | Severity | Result |
|---|---|---|
| **Guide to the Secure Configuration of Red Hat Enterprise Linux 7** 197x fail 20x error 1x unknown 9x notchecked | | |
| **Services** 8x fail 16x error 1x unknown 2x notchecked | | |
| **Obsolete Services** 1x fail 2x notchecked | | |
| **Rlogin, Rsh, and Rexec** 2x notchecked | | |
| Uninstall rsh Package | unknown | pass |
| Disable rlogin Service | high | notchecked |
| Disable rexec Service | high | notchecked |
| Disable rsh Service | high | pass |
| Uninstall rsh-server Package | high | pass |
| Remove Rsh Trust Files | high | pass |
| **Telnet** 1x fail | | |
| Remove telnet Clients | low | fail |
| Disable telnet Service | high | pass |
| Uninstall telnet-server Package | high | pass |
| NIS | | |
| Xinetd | | |
| Chat/Messaging Services | | |
| Cron and At Daemons | | |
| Network Routing | | |
| LDAP | | |
| System Security Services Daemon | | |
| Network Time Protocol | | |
| **Base Services** 1x fail | | |
| Disable KDump Kernel Crash Analyzer (kdump) | medium | fail |
| **NFS and RPC** 3x fail | | |
| Configure NFS Servers | | |
| **Configure NFS Clients** 3x fail | | |
| **Mount Remote Filesystems with Restrictive Options** 3x fail | | |
| Mount Remote Filesystems with Kerberos Security | medium | fail |

| Title | Severity | Result |
|---|---|---|
| Mount Remote Filesystems with nosuid | medium | fail |
| Mount Remote Filesystems with nodev | medium | fail |
| **SSH Server** 3x fail 16x error 1x unknown | | |
| **Configure OpenSSH Server if Necessary** 1x fail 16x error 1x unknown | | |
| Enable Use of Strict Mode Checking | medium | error |
| Disable SSH Support for User Known Hosts | medium | error |
| Disable SSH Access via Empty Passwords | high | error |
| Set SSH Client Alive Count | medium | error |
| Set SSH Idle Timeout Interval | unknown | error |
| Enable SSH Warning Banner | medium | error |
| Use Only FIPS 140-2 Validated MACs | medium | unknown |
| Disable Kerberos Authentication | medium | error |
| Allow Only SSH Protocol 2 | high | pass |
| Disable SSH Support for .rhosts Files | medium | error |
| Disable SSH Support for Rhosts RSA Authentication | medium | pass |
| Do Not Allow SSH Environment Options | medium | error |
| Enable Encrypted X11 Forwarding | high | error |
| Use Only FIPS 140-2 Validated Ciphers | medium | error |
| Disable Host-Based Authentication | medium | error |
| Enable SSH Server firewalld Firewall exception | unknown | fail |
| Enable Use of Privilege Separation | medium | error |
| Disable GSSAPI Authentication | medium | error |
| Disable Compression Or Set Compression to delayed | medium | error |
| Disable SSH Root Login | medium | error |
| Enable the OpenSSH Service | medium | pass |
| Verify Permissions on SSH Server Public *.pub Key Files | medium | fail |
| Verify Permissions on SSH Server Private *_key Key Files | medium | fail |
| **System Settings** 189x fail 4x error 7x notchecked | | |
| **System Accounting with <tt>auditd</tt>** 81x fail | | |
| **Configure <tt>auditd</tt> Data Retention** 8x fail | | |
| Configure auditd flush priority | unknown | fail |
| Configure auditd Max Log File Size | medium | fail |
| Configure auditd mail_acct Action on Low Disk Space | medium | fail |
| Configure auditd space_left Action on Low Disk Space | medium | fail |

| Title | Severity | Result |
|---|---|---|
| Configure auditd to use audispd's syslog plugin | medium | fail |
| Configure auditd admin_space_left Action on Low Disk Space | medium | fail |
| Configure auditd Number of Logs Retained | medium | fail |
| Configure auditd max_log_file_action Upon Reaching Maximum Log Size | medium | fail |
| **Configure <tt>auditd</tt> Rules for Comprehensive Auditing** 72x fail | | |
| **Record Information on Kernel Modules Loading and Unloading** 5x fail | | |
| Ensure auditd Collects Information on Kernel Module Unloading - rmmod | medium | fail |
| Ensure auditd Collects Information on Kernel Module Unloading - delete_module | medium | fail |
| Ensure auditd Collects Information on Kernel Module Loading - insmod | medium | fail |
| Ensure auditd Collects Information on Kernel Module Loading and Unloading - modprobe | medium | fail |
| Ensure auditd Collects Information on Kernel Module Loading - init_module | medium | fail |
| **Record Attempts to Alter Logon and Logout Events** 3x fail | | |
| Record Attempts to Alter Logon and Logout Events - lastlog | medium | fail |
| Record Attempts to Alter Logon and Logout Events - faillock | medium | fail |
| Record Attempts to Alter Logon and Logout Events - tallylog | medium | fail |
| **Records Events that Modify Date and Time Information** 5x fail | | |
| Record Attempts to Alter Time Through stime | unknown | fail |
| Record attempts to alter time through settimeofday | unknown | fail |
| Record Attempts to Alter the localtime File | unknown | fail |
| Record Attempts to Alter Time Through clock_settime | unknown | fail |
| Record attempts to alter time through adjtimex | unknown | fail |
| **Record Events that Modify the System's Discretionary Access Controls** 13x fail | | |
| Record Events that Modify the System's Discretionary Access Controls - fchown | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - setxattr | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - fsetxattr | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - removexattr | medium | fail |
| Record Events that Modify the System's Discretionary Access Controls - fchownat | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - chmod | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - chown | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - fchmod | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - lsetxattr | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - fremovexattr | medium | fail |

| Title | Severity | Result |
|---|---|---|
| Record Events that Modify the System's Discretionary Access Controls - lchown | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - fchmodat | unknown | fail |
| Record Events that Modify the System's Discretionary Access Controls - lremovexattr | medium | fail |
| **Record Execution Attempts to Run SELinux Privileged Commands** 4x fail | | |
| Record Any Attempts to Run setsebool | medium | fail |
| Record Any Attempts to Run semanage | medium | fail |
| Record Any Attempts to Run chcon | medium | fail |
| Record Any Attempts to Run restorecon | medium | fail |
| **Record File Deletion Events by User** 6x fail | | |
| Ensure auditd Collects File Deletion Events by User - rmdir | medium | fail |
| Ensure auditd Collects File Deletion Events by User - unlinkat | medium | fail |
| Ensure auditd Collects File Deletion Events by User | medium | fail |
| Ensure auditd Collects File Deletion Events by User - rename | medium | fail |
| Ensure auditd Collects File Deletion Events by User - renameat | medium | fail |
| Ensure auditd Collects File Deletion Events by User - unlink | medium | fail |
| **Record Information on the Use of Privileged Commands** 17x fail | | |
| Ensure auditd Collects Information on the Use of Privileged Commands - passwd | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - sudo | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - postdrop | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - chsh | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - gpasswd | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - chage | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - userhelper | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - pam_timestamp_check | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - crontab | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - umount | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - unix_chkpwd | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - ssh-keysign | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - sudoedit | medium | fail |

| Title | Severity | Result |
|---|---|---|
| Ensure auditd Collects Information on the Use of Privileged Commands - postqueue | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - su | medium | fail |
| Ensure auditd Collects Information on the Use of Privileged Commands - newgrp | medium | fail |
| ▼ **Record Unauthorized Access Attempts Events to Files (unsuccessful)** 6x fail | | |
| Record Unauthorized Access Attempts to Files (unsuccessful) - truncate | medium | fail |
| Record Unauthorized Access Attempts to Files (unsuccessful) - creat | medium | fail |
| Record Unauthorized Access Attempts to Files (unsuccessful) - open | medium | fail |
| Record Unauthorized Access Attempts to Files (unsuccessful) - open_by_handle_at | medium | fail |
| Record Unauthorized Access Attempts to Files (unsuccessful) - ftruncate | medium | fail |
| Record Unauthorized Access Attempts to Files (unsuccessful) - openat | medium | fail |
| Ensure auditd Collects System Administrator Actions | unknown | fail |
| Record Events that Modify the System's Network Environment | unknown | fail |
| Record Attempts to Alter Process and Session Initiation Information | unknown | fail |
| Make the auditd Configuration Immutable | medium | fail |
| Record Events that Modify User/Group Information - /etc/shadow | medium | fail |
| Ensure auditd Collects Information on Exporting to Media (successful) | medium | fail |
| Record Events that Modify User/Group Information - /etc/security/opasswd | medium | fail |
| System Audit Logs Must Be Owned By Root | medium | pass |
| Record Events that Modify the System's Mandatory Access Controls | unknown | fail |
| Shutdown System When Auditing Failures Occur | medium | fail |
| System Audit Logs Must Have Mode 0640 or Less Permissive | medium | fail |
| Record Events that Modify User/Group Information - /etc/gshadow | medium | fail |
| Record Events that Modify User/Group Information - /etc/passwd | medium | fail |
| Record Events that Modify User/Group Information - /etc/group | medium | fail |
| Enable Auditing for Processes Which Start Prior to the Audit Daemon | medium | fail |
| Enable auditd Service | high | pass |
| ▼ **Configure Syslog** 1x fail | | |
| ▼ **Rsyslog Logs Sent To Remote Host** 1x fail | | |
| Ensure Logs Sent To Remote Host | unknown | fail |
| ▶ Ensure Proper Configuration of Log Files | | |
| ▶ Configure <tt>rsyslogd</tt> to Accept Remote Messages If Acting as a Log Server | | |
| ▼ **Network Configuration and Firewalls** 27x fail 1x error 1x notchecked | | |

| Title | Severity | Result |
|---|---|---|
| **IPv6** 9x fail 1x error | | |
| **Configure IPv6 Settings if Necessary** 7x fail 1x error | | |
| **Disable Automatic Configuration** 7x fail | | |
| Configure Kernel Parameter for Accepting Source-Routed Packets for Interfaces By Default | medium | fail |
| Disable Kernel Parameter for IPv6 Forwarding | medium | fail |
| Configure Kernel Parameter for Accepting IPv6 Source-Routed Packets for All Interfaces | medium | fail |
| Configure Accepting IPv6 Redirects on All Interfaces | medium | fail |
| Configure Accepting IPv6 Router Advertisements by Default | unknown | fail |
| Configure Accepting IPv6 Router Advertisements on All Interfaces | unknown | fail |
| Configure Accepting IPv6 Redirects By Default | medium | fail |
| Use Privacy Extensions for Address | unknown | error |
| **Disable Support for IPv6 Unless Needed** 2x fail | | |
| Disable IPv6 Networking Support Automatic Loading | medium | fail |
| Disable Support for RPC IPv6 | unknown | fail |
| **IPSec Support** 1x notchecked | | |
| Verify Any Configured IPSec Tunnel Connections | medium | notchecked |
| **firewalld** 2x fail | | |
| **Strengthen the Default Ruleset** 1x fail | | |
| Set Default firewalld Zone for Incoming Packets | medium | fail |
| **Inspect and Activate Default firewalld Rules** 1x fail | | |
| Verify firewalld Enabled | medium | fail |
| **Kernel Parameters Which Affect Networking** 12x fail | | |
| **Network Related Kernel Runtime Parameters for Hosts and Routers** 9x fail | | |
| Configure Kernel Parameter for Accepting Source-Routed Packets By Default | medium | pass |
| Configure Kernel Parameter to Ignore Bogus ICMP Error Responses | unknown | fail |
| Configure Kernel Parameter for Accepting ICMP Redirects By Default | medium | fail |
| Configure Kernel Parameter to Use Reverse Path Filtering by Default | medium | pass |
| Configure Kernel Parameter for Accepting Secure Redirects for All Interfaces | medium | fail |
| Configure Kernel Parameter for Accepting IPv4 Source-Routed Packets for All Interfaces | medium | pass |
| Configure Kernel Parameter for Accepting ICMP Redirects for All Interfaces | medium | fail |
| Configure Kernel Parameter to Log Martian Packets | unknown | fail |
| Configure Kernel Parameter to Use Reverse Path Filtering for All Interfaces | medium | pass |

| Title | Severity | Result |
|---|---|---|
| Configure Kernel Parameter for Accepting Secure Redirects By Default | medium | fail |
| Configure Kernel Parameter to Ignore ICMP Broadcast Echo Requests | medium | fail |
| Configure Kernel Parameter to Use TCP Syncookies | medium | fail |
| Configure Kernel Parameter to Log Martian Packets By Default | unknown | fail |
| **Network Parameters for Hosts Only** 3x fail | | |
| Disable Kernel Parameter for IP Forwarding | medium | fail |
| Disable Kernel Parameter for Sending ICMP Redirects for All Interfaces | medium | fail |
| Disable Kernel Parameter for Sending ICMP Redirects by Default | medium | fail |
| **Uncommon Network Protocols** 2x fail | | |
| Disable DCCP Support | medium | fail |
| Disable SCTP Support | medium | fail |
| **Wireless Networking** 2x fail | | |
| **Disable Wireless Through Software Configuration** 2x fail | | |
| Disable Bluetooth Kernel Modules | medium | fail |
| Disable Bluetooth Service | medium | fail |
| Deactivate Wireless Network Interfaces | medium | pass |
| Ensure System is Not Acting as a Network Sniffer | medium | pass |
| **Set Boot Loader Password** 3x notchecked | | |
| Set Boot Loader Password in grub2 | high | pass |
| Verify /boot/grub2/grub.cfg Permissions | medium | notchecked |
| Verify /boot/grub2/grub.cfg User Ownership | medium | notchecked |
| Set the UEFI Boot Loader Password | medium | pass |
| Verify /boot/grub2/grub.cfg Group Ownership | medium | notchecked |
| **SELinux** 1x fail | | |
| SELinux - Booleans | | |
| Ensure SELinux Not Disabled in /etc/default/grub | medium | pass |
| Configure SELinux Policy | high | pass |
| Ensure No Daemons are Unconfined by SELinux | medium | notapplicable |
| Ensure No Device Files are Unlabeled by SELinux | medium | notapplicable |
| Ensure SELinux State is Enforcing | high | fail |
| **Account and Access Control** 28x fail 3x error 1x notchecked | | |
| **Protect Accounts by Restricting Password-Based Login** 5x fail 3x error | | |
| **Set Password Expiration Parameters** 3x fail | | |

| Title | Severity | Result |
|---|---|---|
| Set Password Minimum Length in login.defs | medium | fail |
| Set Password Warning Age | unknown | pass |
| Set Password Minimum Age | medium | fail |
| Set Password Maximum Age | medium | fail |
| **Restrict Root Logins** 3x error | | |
| Restrict Serial Port Root Logins | unknown | error |
| Direct root Logins Not Allowed | medium | error |
| Restrict Virtual Console Root Logins | medium | error |
| Verify Only Root Has UID 0 | high | pass |
| **Set Account Expiration Parameters** 1x fail | | |
| Set Account Expiration Following Inactivity | medium | fail |
| **Verify Proper Storage and Existence of Password Hashes** 1x fail | | |
| Verify All Account Password Hashes are Shadowed | medium | pass |
| Prevent Log In to Accounts With Empty Password | high | fail |
| All GIDs referenced in /etc/passwd must be defined in /etc/group | low | pass |
| **Protect Physical Console Access** 4x fail 1x notchecked | | |
| **Configure Screen Locking** 2x fail | | |
| **Configure Console Screen Locking** 1x fail | | |
| Install the screen Package | medium | fail |
| **Hardware Tokens for Authentication** 1x fail | | |
| Enable Smart Card Login | medium | fail |
| Require Authentication for Single User Mode | medium | pass |
| Disable Ctrl-Alt-Del Burst Action | high | fail |
| Verify that Interactive Boot is Disabled | medium | pass |
| Disable Ctrl-Alt-Del Reboot Activation | high | fail |
| Disable debug-shell SystemD Service | medium | notchecked |
| **Secure Session Configuration Files for Login Accounts** 3x fail | | |
| Ensure that Users Have Sensible Umask Values | | |
| Ensure the Logon Failure Delay is Set Correctly in login.defs | unknown | fail |
| Set Interactive Session Timeout | medium | fail |
| Limit the Number of Concurrent Login Sessions Allowed Per User | low | fail |
| **Warning Banners for System Accesses** 3x fail | | |
| **Implement a GUI Warning Banner** 2x fail | | |
| Enable GNOME3 Login Warning Banner | medium | fail |

| Title | Severity | Result |
|---|---|---|
| Set the GNOME3 Login Warning Banner Text | medium | fail |
| Modify the System Login Banner | medium | fail |
| **Protect Accounts by Configuring PAM** 13x fail | | |
| Set Password Hashing Algorithm | | |
| **Set Lockouts for Failed Password Attempts** 5x fail | | |
| Configure the root Account for Failed Password Attempts | medium | fail |
| Set Lockout Time For Failed Password Attempts | medium | fail |
| Limit Password Reuse | medium | fail |
| Set Interval For Counting Failed Password Attempts | medium | fail |
| Set Deny For Failed Password Attempts | medium | fail |
| **Set Password Quality Requirements** 8x fail | | |
| **Set Password Quality Requirements with pam_pwquality** 8x fail | | |
| Set Password Minimum Length | medium | fail |
| Set Password to Maximum of Consecutive Repeating Characters from Same Character Class | medium | fail |
| Set Password Strength Minimum Digit Characters | medium | fail |
| Set Password Strength Minimum Different Categories | medium | fail |
| Set Password Strength Minimum Different Characters | medium | fail |
| Set Password Strength Minimum Special Characters | medium | fail |
| Set Password Strength Minimum Lowercase Characters | medium | fail |
| Set Password Strength Minimum Uppercase Characters | medium | fail |
| Set Password Retry Prompts Permitted Per-Session | unknown | pass |
| Set Last Logon/Access Notification | low | pass |
| **Installing and Maintaining Software** 39x fail 2x notchecked | | |
| **GNOME Desktop Environment** 23x fail | | |
| **Configure GNOME Screen Locking** 8x fail | | |
| Ensure Users Cannot Change GNOME3 Session Idle Settings | medium | fail |
| Set GNOME3 Screensaver Lock Delay After Activation Period | medium | fail |
| Disable Full User Name on Splash Shield | unknown | fail |
| Ensure Users Cannot Change GNOME3 Screensaver Settings | medium | fail |
| Enable GNOME3 Screensaver Idle Activation | medium | fail |
| Set GNOME3 Screensaver Inactivity Timeout | medium | fail |
| Implement Blank Screensaver | unknown | fail |
| Enable GNOME3 Screensaver Lock After Idle Period | medium | fail |

| Title | Severity | Result |
|---|---|---|
| **GNOME Media Settings** 2x fail | | |
| Disable All GNOME3 Thumbnailers | unknown | fail |
| Disable GNOME3 Automounting | unknown | fail |
| **GNOME System Settings** 3x fail | | |
| Disable Geolocation in GNOME3 | medium | fail |
| Disable Ctrl-Alt-Del Reboot Key Sequence in GNOME3 | high | fail |
| Disable User Administration in GNOME3 | high | fail |
| **Configure GNOME Login Screen** 6x fail | | |
| Enable the GNOME3 Login Smartcard Authentication | medium | fail |
| Disable the GNOME3 Login Restart and Shutdown Buttons | high | fail |
| Disable GDM Automatic Login | high | fail |
| Set the GNOME3 Login Number of Failures | medium | fail |
| Disable the GNOME3 Login User List | medium | fail |
| Disable GDM Guest Login | high | fail |
| **GNOME Network Settings** 2x fail | | |
| Disable WIFI Network Connection Creation in GNOME3 | medium | fail |
| Disable WIFI Network Notification in GNOME3 | medium | fail |
| **GNOME Remote Access Settings** 2x fail | | |
| Require Encryption for Remote Access in GNOME3 | medium | fail |
| Require Credential Prompting for Remote Access in GNOME3 | medium | fail |
| Configure GNOME3 DConf User Profile | high | pass |
| **System and Software Integrity** 12x fail | | |
| Operating System Vendor Support and Certification | | |
| **Federal Information Processing Standard (FIPS)** 2x fail | | |
| Install the dracut-fips Package | medium | fail |
| Enable FIPS Mode in GRUB2 | high | fail |
| **Endpoint Protection Software** 2x fail | | |
| Install Virus Scanning Software | high | fail |
| Install Intrusion Detection Software | high | fail |
| **Software Integrity Checking** 8x fail | | |
| **Verify Integrity with RPM** 1x fail | | |
| Verify and Correct File Permissions with RPM | high | pass |
| Verify File Hashes with RPM | high | fail |
| **Verify Integrity with AIDE** 7x fail | | |

| Title | Severity | Result |
|---|---|---|
| Install AIDE | medium | fail |
| Configure AIDE to Verify Extended Attributes | medium | fail |
| Configure AIDE to Verify Access Control Lists (ACLs) | medium | fail |
| Configure AIDE to Use FIPS 140-2 for Validating Hashes | medium | fail |
| Configure Notification of Post-AIDE Scan Details | medium | fail |
| Configure Periodic Execution of AIDE | medium | fail |
| Build and Test AIDE Database | medium | fail |
| Disable Prelinking | unknown | pass |
| **Updating Software** 4x fail 1x notchecked | | |
| Ensure gpgcheck Enabled For All Yum Package Repositories | high | fail |
| Ensure Software Patches Installed | high | notchecked |
| Ensure Red Hat GPG Key Installed | high | pass |
| Ensure gpgcheck Enabled for Repository Metadata | high | fail |
| Ensure YUM Removes Previous Package Versions | low | fail |
| Ensure gpgcheck Enabled In Main Yum Configuration | high | pass |
| Ensure gpgcheck Enabled for Local Packages | high | fail |
| **Disk Partitioning** 1x notchecked | | |
| Encrypt Partitions | high | notchecked |
| **File Permissions and Masks** 12x fail | | |
| **Verify Permissions on Important Files and Directories** 2x fail | | |
| Ensure All Files Are Owned by a Group | medium | fail |
| Ensure All World-Writable Directories Are Owned by a System Account | unknown | pass |
| Ensure All Files Are Owned by a User | medium | fail |
| **Restrict Dynamic Mounting and Unmounting of Filesystems** 7x fail | | |
| Disable Modprobe Loading of USB Storage Driver | medium | fail |
| Disable Mounting of freevxfs | low | fail |
| Disable Mounting of hfsplus | low | fail |
| Disable Mounting of squashfs | low | fail |
| Disable the Automounter | medium | pass |
| Disable Mounting of jffs2 | low | fail |
| Disable Mounting of hfs | low | fail |
| Disable Mounting of cramfs | low | fail |
| Restrict Partition Mount Options | | |
| **Restrict Programs from Dangerous Execution Patterns** 3x fail | | |

| Title | Severity | Result |
|---|---|---|
| ▼ **Disable Core Dumps** 1x fail | | |
| Disable Core Dumps for SUID programs | unknown | fail |
| ▶ Enable Execute Disable (XD) or No Execute (NX) Support on x86 Systems | | |
| ▼ **Enable ExecShield** 1x fail | | |
| Enable ExecShield via sysctl | medium | pass |
| Enable Randomized Layout of Virtual Address Space | medium | fail |
| Restrict Access to Kernel Message Buffer | unknown | fail |

Show all result details



Generated using OpenSCAP 1.2.17