


# VOSS Insights
# Insights Security

Release 25.1

March 26, 2025

## Legal Information



DOCUMENT ID: 20250326135132

# Contents

# 1. What's New

## 1.1. Insights Security: Release 25.1

- EKB-22636: Investigate Tenable Scan SSL/TLS Forward Secrecy Cipher Suites Not Supported. See: *SSL Ciphers*

  Added steps to enable TLSv1.2 if required. This is disabled by default on Insights 25.1.

# 2. System Security

## 2.1. Security Overview

The platform is not installed with antivirus software or an index of whitelisted applications. The functionality provided by these anti-malware measures is implemented by means of an extensive number of measures to lock down and harden the operating system, platform system and network.

Security covers areas such as application and operating system security updates, operating system hardening, file and application encryption, jailed environments for applications, firewalls and user security. This locked down system ensures that platform users cannot install their own packages, binaries, or applications on the system to perform any malicious actions or allow the exploitation of vulnerabilities (such as Meltdown/Spectre).

---

**Note:** Since the application runs in a virtual environment it is important that the underlying VM infrastructure stays up to date to be protected against any vulnerabilities that may compromise the Virtual Machine on the infrastructure.

---

## 2.2. Security Patches and Updates

Security updates are done with every software release.

### 2.2.1. Restricted User Shell

The platform attempts to reduce the risk of unintentional harm to the operation of the software by restricting the actions users can take. This is done using a specially configured setup of the well-known and actively maintained rbash shell.

The shell actively prevents the following:

- Users cannot set environment variables or alter their command path.
- Users cannot change the current directory.
- Users cannot specify a path to a command to run.

The commands users thus are able to run is only what is allowed by the platform setup. The vast majority of these commands use a common execution interface designed to allow only enough privileges to perform the system administration tasks they are created for. The exact list of commands a user can run is determined by his specific privileges and the specific setup of the machine on which he is working (different applications

can add their own additional commands). This list is displayed on login and can be redisplayed with the **help** command.

## 2.3. Security and Security Policy Management

Upon installation, user passwords are restricted as follows:

- Password length : 8
- Minimum number of days between password change : 1
- Maximum number of days between password change : 60
- Number of days of warning before password expires : 14
- Number number of days between password change: 10

User password and account security settings and policy details can also be configured.

## 2.4. Creating Additional Users

The system ships with the following user accounts:

- `root` – ssh root is disabled. Gaining root access can only be done with a VOSS employee present.
- `admin` – ssh is allowed however, the admin user does not have a shell. When logging in with admin, you are immediately presented with a menu.
- `drop` – ssh is not allowed, only sftp.

  **Note:** The username for the drop account is “drop”. By default no password is set up. You can set the password via the CLI Administration menu (Change Dropbox Password).

- `sysadmin` – ssh is allowed but access is restricted only via a rbash shell.

The system does not allow you to create any additional users.

## 2.5. Creating and Managing SFTP Users

The `drop` user can be used to sftp files to the box. The `drop` password can be set up and changed via the Administration menu.

**Note:** The username for the drop account is “drop”. By default no password is set up. You can set the password via the CLI Administration menu (Change Dropbox Password).


## 2.6. SSH key management

SSH authentication requires maintaining the system SSH keys. This can be configured through the admin menu.

# 3. Network Security

## 3.1. Ports

This table includes connectivity requirements between Insights Arbitrator, Reporting Dashboard, as well as connectivity between these and the following: VOSS Automate, NTP, DNS and AD.

| Source | Destination | Port / protocol | Notes |
|---|---|---|---|
| Arbitrator Server / Dashboard Server | Arbitrator Server / Dashboard Server | 5432, 5433, 5000, 60514, 64514, 64515, 65515, 65516, 64005, 64004, 62009, 62010 (all TCP) | Note: Intra-system communication and queries – Bi-directional |
| Arbitrator Server | Arbitrator Server | 62002, 62003, 62004, 62005, 62006, 11501,30501, 30503, 40501, 40503 (all TCP) | Note: VOSS Fabric TLS tunnel Connection Ports – Bi-directional between Customer systems and NOC systems for event forwarding |
| Arbitrator Server / Dashboard Server | Network Resources (NTP, DNS) | 53, 123 UDP | Time and DNS |
| Client PC – GUI Interface and CLI Management Access | Arbitrator Server / Dashboard Server | 443, 8443, 22, 80 TCP | User Interface Access |
| VOSS Automate | Dashboard Server | 27020 | Database access |
| Arbitrator Server / Dashboard Server | AD | 389 636 TCP UDP | Authentication |

## 3.2. Web Certificate Setup Options

The platform installs a self-signed certificate for the web-frontend by default. This provides encryption of the web-traffic but does not provide users with valid authentication that the server is correct or protect against man-in-the-middle attacks. Customer can install their own certificates through the admin menu.

**Note:**

- Only one certificate file can be installed on the platform.

- Please note the importance of ensuring that SSL certificates generated match the assigned network name of the platform.

# 3.3. SSL Ciphers

## 3.3.1. SSL Ciphers

### Supported SSL Ciphers

This topic lists the SSL ciphers that Insights can support:

**Note:** The OpenSSL software package defines the ciphers Insights (and all Linux distributions) can use. This list may change as ciphers are added or found to be insecure. The Apache application can be configured to use a subset of the base supported ciphers - cipher support can be customized depending on your security requirements.

```
AES256-GCM-SHA384
AES128-GCM-SHA256
AES256-SHA256
AES128-GCM-SHA256
AES256-SHA
AES128-GCM-SHA256
DHE-PSK-CHACHA20-POLY1305
DHE-PSK-AES256-GCM-SHA384
DHE-PSK-AES128-GCM-SHA256
DHE-RSA-CHACHA20-POLY1305
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES256-SHA256
DHE-RSA-AES128-SHA256
DHE-PSK-AES256-CBC-SHA384
DHE-PSK-AES256-CBC-SHA
DHE-PSK-AES128-CBC-SHA256
DHE-PSK-AES128-CBC-SHA
DHE-RSA-AES256-SHA
DHE-RSA-AES128-SHA
ECDHE-PSK-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES128-SHA256
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES128-SHA256
```

(continues on next page)

(continued from previous page)

```
ECDHE-PSK-AES256-CBC-SHA384
ECDHE-PSK-AES256-CBC-SHA
ECDHE-PSK-AES128-CBC-SHA256
ECDHE-PSK-AES128-CBC-SHA
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES128-SHA
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES128-SHA
PSK-CHACHA20-POLY1305
PSK-AES256-GCM-SHA384
PSK-AES128-GCM-SHA256
PSK-AES256-CBC-SHA384
PSK-AES256-CBC-SHA
PSK-AES128-CBC-SHA256
PSK-AES128-CBC-SHA
RSA-PSK-CHACHA20-POLY1305
RSA-PSK-AES256-GCM-SHA384
RSA-PSK-AES128-GCM-SHA256
RSA-PSK-AES256-CBC-SHA384
RSA-PSK-AES256-CBC-SHA
RSA-PSK-AES128-CBC-SHA256
RSA-PSK-AES128-CBC-SHA
SRP-AES-256-CBC-SHA
SRP-AES-128-CBC-SHA
SRP-RSA-AES-256-CBC-SHA
SRP-RSA-AES-128-CBC-SHA
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
```

### Enable/Disable TLSv1.2

Starting with Insights 25.1, TLSv1.2 is disabled by default as the Tenable web application scan flags a number of SSL/TLS ciphers as unsupported due to a medium risk security vulnerability. Disabling TLSv1.2 on Insights disables cipher suites without forward secrecy and retains only cipher suites that provide forward secrecy (ECDHE or DHE based cipher suites).

When TLSv1.2 is disabled, only TLSv1.3 ciphers are present.

---

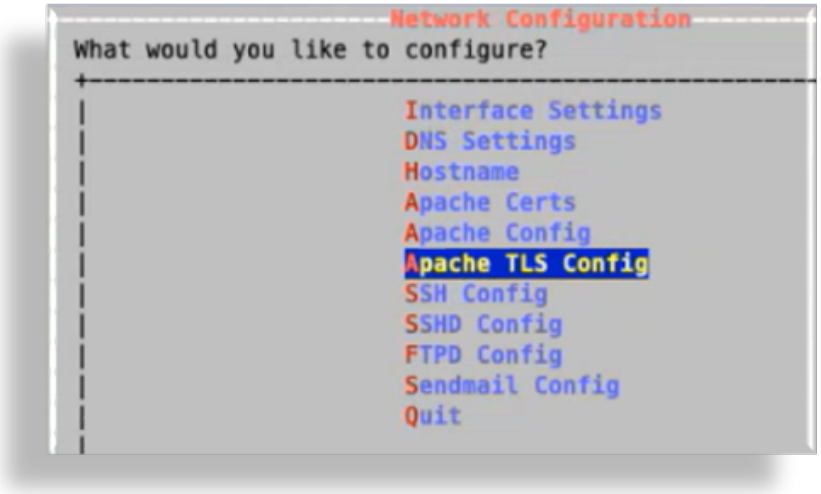
**Note:** This issue is relevant for all Insights products - Arbitrator, Dashboard, DS9.

---

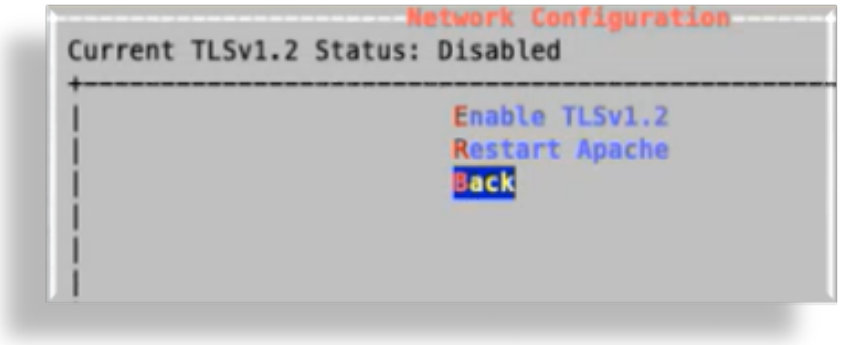
Ciphers offering forward secrecy (FS), also known as perfect forward secrecy (PFS), provide assurances the session keys won't be compromised even if the server's private key is compromised.

If you wish to enable TLSv1.2:

1. Log in on Insights CLI to the **Administration** menu.
2. Select **Apache TLS Config**.




3. On the Apache TLS settings screen, view the current status of TLSv1.2 (enabled or disabled).




4. To enable TLSv1.2, select **Enable TLSv1.2**, then click **OK**.

   Enabling TLSv1.2 allows Insights to support additional ciphers.

   Apache restarts automatically any time you enable or disable TLSv1.2. If you want to restart Apache manually, you can select **Restart Apache** on the TLSv1.2 configuration screen, or on the main **Network Configuration** screen.

## 3.4. Web Configuration

The platform uses Apache as its web server. The configuration has been updated to secure the web server.

The system's cipher configuration has been updated to only support "high" encryption cipher suites. This currently means those with key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

For details, refer to the **Apache Config** menu option upon installation or configuration.

See the Install Guides topic: "Deploy and VM Installation Steps".

The table describes how Apache is secured:

| | |
|---|---|
| Apache Modules | Only the necessary modules are installed. Apache is packaged using VOSS's proprietary package manager so that only VOSS can update Apache's configuration.<br>access_compat_module, alias_module, authn_core_module, authz_core_module, authz_host_module, autoindex_module, core_module, deflate_module, dir_module, filter_module, headers_module, http_module, log_config_module, logio_module, mime_magic_module, mime_module, mpm_prefork_module, php5_module, proxy_http_module, proxy_module, proxy_wstunnel_module, qos_module, rewrite_module, session_cookie_module, session_module, setenvif_module, so_module, socache_shmcb_module, ssl_module, unixd_module |
| Privileges, Permissions, and Ownership | The Apache User and Group directives are set to run as a non-root user, "apache". The "apache" user does not have ssh or login access. |
| Core Dump | The CoreDumpDirectory is disabled. |
| OverRide Disabled | OS Root Directory and all other directories has setting: AllowOverride None |
| Features, Content, Options | All directories has setting: Options None |
| Default Content removed | Default HTML and cgi content removed. |
| HTTP Request Methods Restricted | HTTP request methods limited to GET POST OPTIONS |
| HTTP TRACE Method Disabled | TraceEnable off |

| | |
|---|---|
| Force HTTP 1.1 | # Force HTTP 1.1<br>RewriteEngine On<br>RewriteCond %{THE_REQUEST} !HTTP/1.1$<br>RewriteRule .* - [F] |
| HTTP Strict Transport Security | Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" |
| Information Leakage | ServerTokens ProductOnly |
| ServerSignature | ServerSignature Off |
| ETag Response Header | FileETag None |
| Restricted Files | Access to .ht* files are restricted. |
| Ports | Only https port 443 supported. |
| SSL / TLS | TLSv1.2 and TLSv1.3 supported<br>TLSv1.2 is disabled by default on Insights, starting with Insights 25.1. |
| Ciphers | Only HIGH SSLCipherSuite supported |
| Certificates | System is installed with a self signed certificate. Customer may install their own signed certificate through the admin menu. |
| Denial of Service Mitigations | Mod_qos is installed and configured to fight slowloris. |

Tenable.io, nmap vulnerability, and sslcans are consistently updated and run weekly on our product to ensure that we have the best possible settings for our web server.

**Related topics**

- *SSL Ciphers*

## 3.5. Scans

The platform was scanned with an external openscap tool using the DISA STIG specification for RHEL7. Refer to *Scan Results* in this document.

Because our operating system is proprietary, there is no specification designed specifically for our operating system so we used the DISA STIG specification for RHEL7 as reference.

Both the openscap tool and the specification are external and not controlled by VOSS.

We also scan our system within VOSS using Tenable.io on a daily basis.

DISA STIG refers to an organization (DISA — Defense Information Systems Agency) that provides technical guides (STIG — Security Technical Implementation Guide).

The Rhel7 specification we used was provided by the Defense Information Systems Agency.

Many of the modules could not be validated as the operating system is not Redhat

# 4. Packages

Refer to the VOSS Insights Open Source License Usage document for the list of packages, versions and licenses used in VOSS Insights.

# 5. Scan Results

The tables below show the scan results of the external openscap tool using the DISA STIG specification for RHEL7.

Where the result is False, Unknown or Error, the **Response** column provides details.

## 5.1. False

Table 1: False

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:95733 | | The Red Hat Enterprise Linux operating system must label all off-loaded audit logs before sending them to the central log server. | Not supported. |
| oval:mil.disa.stig.rhel7:def:95731 | | The Red Hat Enterprise Linux operating system must take appropriate action when the audisp-remote buffer is full. | Not supported. |
| oval:mil.disa.stig.rhel7:def:95729 | | The Red Hat Enterprise Linux operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon. | Not supported. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:95715 | | Verify /etc/pam.d/system-auth is included in /etc/pam.d/passwd | Pam module not installed. |
| oval:mil.disa.stig.rhel7:def:93705 | | Audit Kernel Module Creation - create _module | Kernel does not support modules. |
| oval:mil.disa.stig.rhel7:def:92521 | | RHEL-07-040201 - The Red Hat Enterprise Linux operating system must implement virtual address space randomization. | ASLR is enabled. |
| oval:mil.disa.stig.rhel7:def:92519 | | Require authentication upon booting into single-user and maintenance modes. | Password is required. |
| oval:mil.disa.stig.rhel7:def:92517 | | Disable dccp Kernel Module | DCCP is not enabled. |
| oval:mil.disa.stig.rhel7:def:885 | [CCE-27394-6] [auditd _data _retention _action _mail _acct] | Auditd Email Account to Notify Upon Action | Auditd is not installed. |
| oval:mil.disa.stig.rhel7:def:87815 | | The Red Hat Enterprise Linux operating system must be configured so that the audit system takes appropriate action when there is an error sending audit records to a remote system. | Not supported. |
| oval:mil.disa.stig.rhel7:def:878 | [CCE-80431-0] [audit _rules _usergroup _modification _shadow] | Audit User/Group Modification (/etc/shadow) | Root readable writable. |
| oval:mil.disa.stig.rhel7:def:875 | [CCE-80435-1] [audit _rules _usergroup _modification _passwd] | Audit User/Group Modification (/etc/passwd) | Root readable writable. |
| oval:mil.disa.stig.rhel7:def:872 | [CCE-80430-2] [audit _rules _usergroup _modification _opasswd] | Audit User/Group Modification (opasswd) | Not supported. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:87057 | | The Red Hat Enterprise Linux operating system must implement certificate status checking for PKI authentication. | Pam module not installed. |
| oval:mil.disa.stig.rhel7:def:86943 | | The ipv6.disable Kernel Boot Option Check | Not disabled. |
| oval:mil.disa.stig.rhel7:def:869 | [CCE-80432-8] [audit _rules _usergroup _modification _gshadow] | Audit User/Group Modification (gshadow) | Not supported. |
| oval:mil.disa.stig.rhel7:def:86815 | | Ensure auditd Collects Information on the Use of Privileged Commands - kmod | Auditd is not installed. |
| oval:mil.disa.stig.rhel7:def:86765 | | Record Any Attempts to Run setfiles | setfiles not installed. |
| oval:mil.disa.stig.rhel7:def:86715 | | The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached. | Not supported. |
| oval:mil.disa.stig.rhel7:def:86711 | | The audit system must take appropriate action when the audit storage volume is full. | System has various logrotation policies, db deletion policies to help keeping disk not full. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:86709 | | The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited. | Auditd is not installed. |
| oval:mil.disa.stig.rhel7:def:86707 | | The operating system must off-load audit records onto a different system or media from the system being audited. | Not supported. |
| oval:mil.disa.stig.rhel7:def:86703 | [CCE-27407-6] | The audit service must be running. | Not supported. |
| oval:mil.disa.stig.rhel7:def:86689 | [CCE-27173-4] | The system must use a separate file system for /tmp (or equivalent). | Not supported. |
| oval:mil.disa.stig.rhel7:def:86639 | | The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are defined in the /etc/passwd file. | True. No additional uses may be added to system. |
| oval:mil.disa.stig.rhel7:def:866 | [CCE-80433-6] [audit _rules _usergroup _modification _group] | Audit User/Group Modification (/etc/group) | Root readable writable. |
| oval:mil.disa.stig.rhel7:def:86555 | | Passwords must be restricted to a 60-day maximum lifetime. | Not supported. No additional users may be added to the system. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:805 | [CCE-80386-6] [audit _rules _unsuccessful _file _modification _open] [audit _rules _unsuccessful _file _modification _open] | RHEL-07-030510 - The Red Hat Enterprise Linux operating system must audit all uses of the creat, open, openat, open _by _handle _at, truncate and ftruncate syscalls. | Commands not installed. |
| oval:mil.disa.stig.rhel7:def:776 | [CCE-80381-7] [audit _rules _system _shutdown] | Shutdown System When Auditing Failures Occur | Not supported. |
| oval:mil.disa.stig.rhel7:def:773 | [CCE-27461-3] [audit _rules _sysadmin _actions] | Audit System Administrator Actions | System Administrator is restricted through admin shell. |
| oval:mil.disa.stig.rhel7:def:763 | [CCE-80399-9] [audit _rules _privileged _commands _userhelper] | Ensure auditd Collects Information on the Use of Privileged Commands - userhelper | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:760 | [CCE-80396-5] [audit _rules _privileged _commands _unix _chkpwd] | Ensure auditd Collects Information on the Use of Privileged Commands - unix _chkpwd | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:757 | [CCE-80405-4] [audit _rules _privileged _commands _umount] | Ensure auditd Collects Information on the Use of Privileged Commands - umount | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:751 | [CCE-80401-3] [audit _rules _privileged _commands _sudo] | Ensure auditd Collects Information on the Use of Privileged Commands - sudo | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:748 | [CCE-80400-5] [audit _rules _privileged _commands _su] | Ensure auditd Collects Information on the Use of Privileged Commands - su | Not supported. Only available to root. Root account is restricted. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:745 | [CCE-80408-8] [audit _rules _privileged _commands _ssh _keysign] | Ensure auditd Collects Information on the Use of Privileged Commands - ssh _keysign | Not supported. |
| oval:mil.disa.stig.rhel7:def:739 | [CCE-80407-0] [audit _rules _privileged _commands _postqueue] | Ensure auditd Collects Information on the Use of Privileged Commands - postqueue | Not supported. |
| oval:mil.disa.stig.rhel7:def:736 | [CCE-80406-2] [audit _rules _privileged _commands _postdrop] | Ensure auditd Collects Information on the Use of Privileged Commands - postdrop | Not supported. |
| oval:mil.disa.stig.rhel7:def:733 | [CCE-80395-7] [audit _rules _privileged _commands _passwd] | Ensure auditd Collects Information on the Use of Privileged Commands - passwd | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:730 | [CCE-80411-2] [audit _rules _privileged _commands _pam _timestamp _check] | Ensure auditd Collects Information on the Use of Privileged Commands - pam _timestamp _check | Not supported. |
| oval:mil.disa.stig.rhel7:def:727 | [CCE-80403-9] [audit _rules _privileged _commands _newgrp] | Ensure auditd Collects Information on the Use of Privileged Commands - newgrp | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:724 | [CCE-80397-3] [audit _rules _privileged _commands _gpasswd] | Ensure auditd Collects Information on the Use of Privileged Commands - gpasswd | Not supported. Only available to root. Root account is restricted. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:721 | [CCE-80410-4] [audit _rules _privileged _commands _crontab] | Ensure auditd Collects Information on the Use of Privileged Commands - crontab | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:718 | [CCE-80404-7] [audit _rules _privileged _commands _chsh] | Ensure auditd Collects Information on the Use of Privileged Commands - chsh | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:715 | [CCE-80398-1] [audit _rules _privileged _commands _chage] | Ensure auditd Collects Information on the Use of Privileged Commands - chage | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:710 | [audit _rules _privileged _commands] | The Red Hat EnterpriseLinux Operating system must audit all executions of privileged functions. | Not supported. |
| oval:mil.disa.stig.rhel7:def:686 | [CCE-27447-2] [audit _rules _media _export] | The Red Hat Enterprise Linux operating system must audit all uses of the mount command and syscall. | Not supported. |
| oval:mil.disa.stig.rhel7:def:676 | [CCE-80384-1] [audit _rules _login _events _lastlog] | Record Attempts to Alter Login and Logout Events - lastlog | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:675 | [CCE-80383-3] [audit _rules _login _events _faillock] | Record Attempts to Alter Login and Logout Events - faillock | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:658 | [CCE-80415-3] [audit _rules _kernel _module _loading _delete] | Audit Kernel Module Loading and Unloading - delete _module | Not supported. Command not installed. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:657 | [CCE-80414-6] [audit _rules _kernel _module _loading _init] | RHEL-07-030820 - The Red Hat Enterprise Linux operating system must audit all uses of the init _module and finit _module syscalls. | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:626 | [CCE-27206-2] [audit _rules _file _deletion _events _unlink] | RHEL-07-030910 - The Red Hat Enterprise Linux operating system must audit all uses of the unlink, unlinkat, rename, renameat and rmdir syscalls. | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:621 | [CCE-80392-4] [audit _rules _execution _setsebool] | Record Any Attempts to Run setsebool | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:618 | [CCE-80391-6] [audit _rules _execution _semanage] | Record Any Attempts to Run semanage | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:612 | [CCE-80393-2] [audit _rules _execution _chcon] | Record Any Attempts to Run chcon | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:607 | [CCE-27213-8] [audit _rules _dac _modification _setxattr] | RHEL-07-030440 - The Red Hat Enterprise Linux operating system must audit all uses of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr and lremovexattr syscalls. | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:552 | [CCE-27364-9] [audit _rules _dac _modification _chown] | RHEL-07-030370 - The Red Hat Enterprise Linux operating system must audit all uses of the chown, fchown, fchownat and lchown syscalls. | Not supported. Only available to root. Root account is restricted. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:546 | [CCE-27339-1] [audit _rules _dac _modification _chmod] | RHEL-07-030410 - The Red Hat Enterprise Linux operating system must audit all uses of the chmod, fchmod and fchmodat syscalls. | Not supported. Only available to root. Root account is restricted. |
| oval:mil.disa.stig.rhel7:def:544 | [audit _rules _augenrules] | Check use of augenrules | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:542 | [audit _rules _auditctl] | Check use of auditctl | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:525 | [CCE-26952-2] [aide _periodic _cron _checking] | Configure Periodic Execution of AIDE | Not supported. Command not installed. |
| oval:mil.disa.stig.rhel7:def:518 | [CCE-80205-8] [accounts _umask _etc _login _defs] | RHEL-07-020240 - The Red Hat Enterprise Linux operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files. | Not supported. No additional users may be added to the system. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:510 | [accounts _tmout] | RHEL-07-040160 - The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with a communication session are terminated at the end of the session or after 15 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements. | Not supported. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:486 | [accounts _password _pam _unix _remember] [CCE-26923-3] | Limit Password Reuse | supported. Only a limited number of accounts on system. |
| oval:mil.disa.stig.rhel7:def:484 | [CCE-27200-5] [accounts _password _pam _ucredit] | Set Password ucredit Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:481 | [CCE-27160-1] [accounts _password _pam _retry] | Set Password retry Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:478 | [CCE-27360-7] [accounts _password _pam _ocredit] | Set Password ocredit Requirements | Not supported. Pam not installed. No additional users may be added to the system. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:476 | [CCE-27293-0] [accounts _password _pam _minlen] | Set Password minlen Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:474 | [CCE-27115-5] [accounts _password _pam _minclass] | Set Password minclass Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:472 | [CCE-27333-4] [accounts _password _pam _maxrepeat] | Set Password maxrepeat Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:470 | [CCE-27512-3] [accounts _password _pam _maxclassrepeat] | The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed the number of repeating characters of the same character class must not be more than four characters. | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:468 | [CCE-27345-8] [accounts _password _pam _lcredit] | Set Password lcredit Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:466 | [CCE-26631-2] [accounts _password _pam _difok] | Set Password difok Requirements | Not supported. Pam not installed. No additional users may be added to the system. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:464 | [accounts _password _pam _pwquality] | Check pam _pwquality Existence in system-auth | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:463 | [CCE-27214-6] [accounts _password _pam _dcredit] | Set Password dcredit Requirements | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:449 | [CCE-27081-9] [accounts _max _concurrent _login _sessions] | Set Maximum Number of Concurrent Login Sessions Per User | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:443 | [CCE-27471-2] [account _disable _post _pw _expiration] | The Red Hat Enterprise Linux operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. | Not supported. Pam not installed. No additional users may be added to the system. |
| oval:mil.disa.stig.rhel7:def:304 | [sysctl _static _net _ipv6 _conf _all _accept _source _route] | Kernel net.ipv6.conf .all.accept _source _route Parameter Configuration Check | net.ipv6.conf .default.accept _source _route = 0 |
| oval:mil.disa.stig.rhel7:def:303 | [CCE-80179-5] [sysctl _net _ipv6 _conf _all _accept _source _route] | Kernel net.ipv6.conf .all.accept _source _route Parameter Configuration and Runtime Check | net.ipv6.conf .default.accept _source _route = 0 |
| oval:mil.disa.stig.rhel7:def:297 | [sysctl _kernel _ipv6 _disable] | Kernel Runtime Parameter IPv6 Check | net.ipv6.conf .all.disable _ipv6 = 0 |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:285 | [sysctl _static _net _ipv4 _icmp _echo _ignore _broadcasts] | Kernel net.ipv4.icmp _echo _ignore _broadcasts Parameter Configuration Check | net.ipv4.icmp _echo _ignore _broadcasts = 1 |
| oval:mil.disa.stig.rhel7:def:284 | [CCE-80165-4] [sysctl _net _ipv4 _icmp _echo _ignore _broadcasts] | Kernel net.ipv4.icmp _echo _ignore _broadcasts Parameter Configuration and Runtime Check | net.ipv4.icmp _echo _ignore _broadcasts = 1 |
| oval:mil.disa.stig.rhel7:def:283 | [sysctl _runtime _net _ipv4 _conf _default _send _redirects] | Kernel net.ipv4.conf .default.send _redirects Parameter Runtime Check | net.ipv4.conf .default.send _redirects = 1 |
| oval:mil.disa.stig.rhel7:def:282 | [sysctl _static _net _ipv4 _conf _default _send _redirects] | Kernel net.ipv4.conf .default.send _redirects Parameter Configuration Check | net.ipv4.conf .default.send _redirects = 1 |
| oval:mil.disa.stig.rhel7:def:281 | [CCE-80156-3] [sysctl _net _ipv4 _conf _default _send _redirects] | Kernel net.ipv4.conf. default.send _redirects Parameter Configuration and Runtime Check | net.ipv4.conf. default.send _redirects = 1 |
| oval:mil.disa.stig.rhel7:def:271 | [sysctl _runtime _net _ipv4 _conf _default _accept _source _route] | Kernel net.ipv4.conf .default.accept _source _route Parameter Runtime Check | net.ipv4.conf .all.accept _source _route = 0 |
| oval:mil.disa.stig.rhel7:def:270 | [sysctl _static _net _ipv4 _conf _default _accept _source _route] | Kernel net.ipv4.conf .default.accept _source _route Parameter Configuration Check | net.ipv4.conf .all.accept _source _route = 0 |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:269 | [CCE-80162-1] [sysctl _net _ipv4 _conf _default _accept _source _route] | Kernel net.ipv4.conf .default.accept _source _route Parameter Configuration and Runtime Check | net.ipv4.conf .all.accept _source _route = 0 |
| oval:mil.disa.stig.rhel7:def:266 | [CCE-80163-9] [sysctl _net _ipv4 _conf _default _accept _redirects] | The Red Hat Enterprise Linux operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted. | net.ipv4.conf .all.accept _redirects = 0 |
| oval:mil.disa.stig.rhel7:def:263 | [CCE-80156-3] [sysctl _net _ipv4 _conf _all _send _redirects] | The Red Hat Enterprise Linux operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. | net.ipv4.conf .all.accept _redirects = 0 |
| oval:mil.disa.stig.rhel7:def:179 | | RHEL-07-010343 - The Red Hat Enterprise Linux operating system must require re-authentication when using the sudo command. | Not applicable. No additional uses may be added to the system. |
| oval:mil.disa.stig.rhel7:def:178 | | RHEL-07-010342 - The Red Hat Enterprise Linux operating system must use the invoking user password for privilege escalation when using sudo. | Not applicable. No additional uses may be added to the system. |
| oval:mil.disa.stig.rhel7:def:176 | [CCE-80351-0] [sudo _remove _nopasswd] | Ensure NOPASSWD Is Not Used in Sudo | sudoers file is not editable without root access. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:169 | [CCE-80349-4] | RHEL-07-020250 - The Red Hat Enterprise Linux operating system must be a vendor supported release | Not Red Hat. |
| oval:mil.disa.stig.rhel7:def:1428 | [system _info _architecture _ppc _64] | Test for PPC and PPCLE Architecture | Not supported. |
| oval:mil.disa.stig.rhel7:def:1417 | [sysctl _runtime _net _ipv6 _conf _all _disable _ipv6] | Kernel net.ipv6.conf .all.disable _ipv6 Parameter Runtime Check | net.ipv6.conf .all.disable _ipv6 = 0 |
| oval:mil.disa.stig.rhel7:def:1416 | [sysctl _static _net _ipv6 _conf _all _disable _ipv6] | Kernel net.ipv6.conf .all.disable _ipv6 Parameter Configuration Check | net.ipv6.conf .all.disable _ipv6 = 0 |
| oval:mil.disa.stig.rhel7:def:1405 | [CCE-80437-7] [sssd _enable _pam _services] | Configure PAM in SSSD Services | Pam module not installed. |
| oval:mil.disa.stig.rhel7:def:1367 | [CCE-27104-9] [set _password _hashing _algorithm _systemauth] | Set Password Hashing Algorithm in /etc/pam.d/system-auth | Pam module not installed. |
| oval:mil.disa.stig.rhel7:def:1363 | [CCE-27053-8] [set _password _hashing _algorithm _libuserconf] | Set SHA512 Password Hashing Algorithm in /etc/libuser.conf | Pam module not installed. |
| oval:mil.disa.stig.rhel7:def:1319 | [CCE-26971-2] [partition _for _var _log _audit] | Ensure /var/log/audit Located On Separate Partition | Not applicable. |
| oval:mil.disa.stig.rhel7:def:1315 | [CCE-26404-4] [partition _for _var] | Ensure /var Located On Separate Partition | Not applicable. |
| oval:mil.disa.stig.rhel7:def:1311 | [CCE-80144-9] [partition _for _home] | Ensure /home Located On Separate Partition | Not applicable. |
| oval:mil.disa.stig.rhel7:def:126 | [CCE-80359-3] [grub2 _enable _fips _mode] | Enable FIPS Mode in GRUB2 | |
| oval:mil.disa.stig.rhel7:def:1141 | [kernel _module _usb-storage _disabled] | Disable usb-storage Kernel Module | Kernel does not support modules. |

**continues on next page**

**Table 1 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:1117 | [CCE-27503-2] [gid _passwd _group _same] | All GIDs Are Present In /etc/group | 1 |
| oval:mil.disa.stig.rhel7:def:110 | [CCE-80347-8] [ensure _gpgcheck _local _packages] | Ensure gpgcheck Enabled for Local Packages | gpgcheck not supported. |
| oval:mil.disa.stig.rhel7:def:108 | [CCE-80346-0] [clean _components _post _updating] | Ensure YUM Removes Previous Package Versions | YUM is not supported. |
| oval:mil.disa.stig.rhel7:def:1027 | [CCE-26989-4] [ensure _gpgcheck _globally _activated] | Ensure Yum gpgcheck Globally Activated | YUM is not supported. |
| oval:mil.disa.stig.rhel7:def:1020 | [display _login _attempts] | The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon logon. | 1 |

## 5.2. Unknown

Table 2: Unknown

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:999 | [CCE-80371-8] | Gnome lock-delay setting lock | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:988 | [CCE-80112-6] [dconf _gnome _screensaver _lock _enabled] | Enable GNOME3 Screensaver Lock After Idle Period | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:985 | [CCE-80370-0] [dconf _gnome _screensaver _lock _delay] | Enable GNOME3 Screensaver Lock Delay After Idle Period | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:981 | [CCE-80110-0] [dconf _gnome _screensaver _idle _delay] | Configure the GNOME3 GUI Screen locking | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:978 | [CCE-80111-8] [dconf _gnome _screensaver _idle _activation _enabled] | Enable GNOME3 Screensaver Idle Activation | Gnome or X11 UI package not installed. |

**continues on next page**

**Table 2 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:93703 | [package _vsftpd _removed] | The operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface. | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:92515 | | Smartcard authentication enabled for graphical user logon. | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:924 | [enable _dconf _user _profile] | Implement Local DB for DConf User Profile | Not applicable. |
| oval:mil.disa.stig.rhel7:def:923 | [package _dconf _installed] | Package dconf Installed | Not applicable. |
| oval:mil.disa.stig.rhel7:def:922 | [CCE-26970-4] [dconf _gnome _banner _enabled] | Enable GNOME3 Login Warning Banner | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:87041 | | The operating system must have the required packages for multifactor authentication installed. | Multifactor not supportted. |
| oval:mil.disa.stig.rhel7:def:86875 | | Package openssh-server is version 7.4 or higher | openssh 9.0 installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:526 | [package _aide _installed] | Package aide Installed | Not installed. |
| oval:mil.disa.stig.rhel7:def:4248 | [package _openssh-server _installed] [CCE-80215-7] | Package openssh-server Installed | openssh 9.0 installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:171 | [CCE-80223-1] [sshd _use _priv _separation] | Use Privilege Separation | UsePrivilegeSeparation yes |

**continues on next page**

**Table 2 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:168 | [CCE-27455-5] [sshd _use _approved _macs] | RHEL-07-040400 - The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms | Configurable by customer through admin ui. |
| oval:mil.disa.stig.rhel7:def:166 | [CCE-80225-6] [sshd _print _last _log] | The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon SSH logon. | 1 |
| oval:mil.disa.stig.rhel7:def:164 | [CCE-80222-3] [sshd _enable _strictmodes] | Enable SSH Server Strict Mode | StrictModes yes |
| oval:mil.disa.stig.rhel7:def:162 | [CCE-80221-5] [sshd _disable _kerb _auth] | Disable Kerberos Authentication | Configurable by customer through admin ui. |
| oval:mil.disa.stig.rhel7:def:160 | [CCE-80220-7] [sshd _disable _gssapi _auth] | Disable GSSAPI Authentication | Configurable by customer through admin ui. |
| oval:mil.disa.stig.rhel7:def:156 | [package _openssh-server _removed] | Package openssh-server Removed | openssh 9.0 installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1399 | [CCE-27295-5] [sshd _use _approved _ciphers] | RHEL-07-040110 - The Red Hat Enterprise Linux 7 operating system must implement DoD-approved encryption to protect the confidentiality of SSH connections | Configurable by customer through admin ui. |

**continues on next page**

**Table 2 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:1393 | [CCE-27082-7] [sshd _set _keepalive] | Set ClientAlive-CountMax for User Logins | ClientAliveInterval 600 |
| oval:mil.disa.stig.rhel7:def:1389 | [CCE-80226-4] [sshd _enable _forwarding] | RHEL-07-040710 - Disable X11 Forwarding | Gnome or X11 UI package not installed. |
| oval:mil.disa.stig.rhel7:def:1385 | [CCE-27363-1] [sshd _do _not _permit _user _env] | Do Not Allow Users to Set Environment Options | X11Forwarding no |
| oval:mil.disa.stig.rhel7:def:1383 | [CCE-80372-6] [sshd _disable _user _known _hosts] | Disable SSH Support for User Known Hosts | IgnoreUser-KnownHosts no |
| oval:mil.disa.stig.rhel7:def:1381 | [CCE-27445-6] [sshd _disable _root _login] | Disable root Login via SSH | Root ssh not supportted. |
| oval:mil.disa.stig.rhel7:def:1379 | [CCE-80373-4] [sshd _disable _rhosts _rsa] | Disable SSH Support for Rhosts RSA Authentication | RhostsRSAAu-thentication no |
| oval:mil.disa.stig.rhel7:def:1377 | [CCE-27377-1] [sshd _disable _rhosts] | Disable .rhosts Files | IgnoreRhosts yes |
| oval:mil.disa.stig.rhel7:def:1340 | [CCE-27157-7] [rpm _verify _hashes] | Verify File Hashes with RPM | RPM not supporttted |
| oval:mil.disa.stig.rhel7:def:1309 | [CCE-27399-5] [package _ypserv _removed] | Package ypserv Removed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1305 | [CCE-27218-7] [package _xorg-x11-server-common _removed] | Package xorg-x11-server-common Removed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1301 | [package _vsftpd _removed] | Package vsftpd Removed | vsftpd required for some customers. |
| oval:mil.disa.stig.rhel7:def:1296 | [CCE-80213-2] [package _tftp-server _removed] | Package tftp-server Removed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1292 | [package _telnet-server _removed] [CCE-27165-0] | Package telnet-server Removed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:128 | [package _dracut-fips _installed] | Package dracut-fips Installed | Package not installed. (See open source package listing) |

**continues on next page**

**Table 2 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:1271 | [CCE-27342-5] [package _rsh-server _removed] | Package rsh-server Removed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:127 | [disable _prelink] | Disable Prelinking | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1264 | [package _net-snmp _removed] | Package net-snmp Removed | net-snmp required for some customers. |
| oval:mil.disa.stig.rhel7:def:1122 | [CCE-80105-0] [gnome _gdm _disable _guest _login] | Disable GDM Guest Login | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1120 | [package _gdm _installed] | Package gdm Installed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1119 | [CCE-80104-3] [gnome _gdm _disable _automatic _login] | Disable GDM Automatic Login | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1017 | [package _prelink _removed] | Package prelink Removed | Package not installed. (See open source package listing) |
| oval:mil.disa.stig.rhel7:def:1011 | [CCE-27413-4] [disable _host _auth] | Disable Host-Based Authentication | Pam module not installed. |
| oval:mil.disa.stig.rhel7:def:1 | [cpe:/o:redhat:enterprise _linux:7] [installed _OS _is _rhel7] | Red Hat Enterprise Linux 7 | Not Red Hat. |

## 5.3. Error

Table 3: Error

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:455 | [CCE-27002-5] [accounts _minimum _age _login _defs] | Set Password Expiration Parameters | Default settings. No additional users may be added. |

**continues on next page**

**Table 3 – continued from previous page**

| ID | Reference ID | Title | Response |
|---|---|---|---|
| oval:mil.disa.stig.rhel7:def:453 | [CCE-27051-2] [accounts _maximum _age _login _defs] | Set Password Expiration Parameters | Default settings. No additional users may be added. |
| oval:mil.disa.stig.rhel7:def:305 | [sysctl_runtime _net _ipv6 _conf _all _accept _source _route] | Kernel net.ipv6.conf .all.accept _source _route Parameter Runtime Check | net.ipv4.conf .all.accept _source _route = 0 |
| oval:mil.disa.stig.rhel7:def:286 | [sysctl _runtime _net _ipv4 _icmp _echo _ignore _broadcasts] | Kernel net.ipv4.icmp _echo _ignore _broadcasts Parameter Runtime Check | net.ipv4.icmp _echo _ignore _broadcasts = 1 |
| oval:mil.disa.stig.rhel7:def:1391 | [CCE-27433-2] [sshd _set _idle _timeout] | Set OpenSSH Idle Timeout Interval | ClientAliveInterval 600 |
| oval:mil.disa.stig.rhel7:def:101 | [CCE-80352-8] [accounts _logon _fail _delay] | Ensure that FAIL_DELAY is Configured in /etc/login.defs | FAIL_DELAY 3 |

## 5.4. True

No response provided.

Table 4: True

| ID | Reference ID | Title |
|---|---|---|
| oval:mil.disa.stig.rhel7:def:95719 | [CCE-80354-4] | Set the UEFI Boot Loader Password |
| oval:mil.disa.stig.rhel7:def:95717 | [CCE-27309-4] | Set Boot Loader Password (BIOS) for RHEL 7.2 and up |
| oval:mil.disa.stig.rhel7:def:86903 | | There must be no shosts.equiv files on the system. |
| oval:mil.disa.stig.rhel7:def:86901 | | There must be no .shosts files on the system. |
| oval:mil.disa.stig.rhel7:def:86635 | | The Red Hat Enterprise Linux operating system must be configured so that all local interactive users have a home directory assigned in the /etc/passwd file. |

**continues on next page**

**Table 4 – continued from previous page**

| ID | Reference ID | Title |
|---|---|---|
| oval:mil.disa.stig.rhel7:def:86609 | [CCE-27498-5] | File system automounter must be disabled unless required. |
| oval:mil.disa.stig.rhel7:def:86551 | | Passwords must be restricted to a 1 day minimum lifetime. |
| oval:mil.disa.stig.rhel7:def:548 | [system _info _architecture _64bit] | Test for 64-bit Architecture |
| oval:mil.disa.stig.rhel7:def:457 | [CCE-27175-9] [accounts _no _uid _except _zero] | UID 0 Belongs Only To Root |
| oval:mil.disa.stig.rhel7:def:447 | [CCE-80434-4] [accounts _have _homedir _login _defs] | Ensure new users receive home directories |
| oval:mil.disa.stig.rhel7:def:292 | [sysctl _runtime _net _ipv4 _ip _forward] | Kernel net.ipv4.ip _forward Parameter Runtime Check |
| oval:mil.disa.stig.rhel7:def:291 | [sysctl _static _net _ipv4 _ip _forward] | Kernel net.ipv4.ip _forward Parameter Configuration Check |
| oval:mil.disa.stig.rhel7:def:290 | [CCE-80157-1] [sysctl _net _ipv4 _ip _forward] | Kernel net.ipv4.ip _forward Parameter Configuration and Runtime Check |
| oval:mil.disa.stig.rhel7:def:251 | [CCE-27434-0] [sysctl _net _ipv4 _conf _all _accept _source _route] | Kernel net.ipv4.conf.all.accept _source _route Parameter Configuration and Runtime Check |
| oval:mil.disa.stig.rhel7:def:250 | [sysctl _runtime _net _ipv4 _conf _all _accept _redirects] | Kernel net.ipv4.conf.all.accept _redirects Parameter Runtime Check |
| oval:mil.disa.stig.rhel7:def:249 | [sysctl _static _net _ipv4 _conf _all _accept _redirects] | Kernel net.ipv4.conf.all.accept _redirects Parameter Configuration Check |
| oval:mil.disa.stig.rhel7:def:248 | [CCE-80158-9] [sysctl _net _ipv4 _conf _all _accept _redirects] | Kernel net.ipv4.conf.all.accept _redirects Parameter Configuration and Runtime Check |
| oval:mil.disa.stig.rhel7:def:177 | | RHEL-07-010341 - The Red Hat Enterprise Linux operating system must restrict privilege elevation to authorized personnel. |
| oval:mil.disa.stig.rhel7:def:173 | [CCE-80350-2] [sudo _remove _no _authenticate] | Ensure !authenticate Is Not Used in Sudo |
| oval:mil.disa.stig.rhel7:def:158 | [CCE-80224-9] [sshd _disable _compression] | Disable Compression Or Set Compression to delayed |
| oval:mil.disa.stig.rhel7:def:1427 | [system _info _architecture _x86 _64] | Test for x86 _64 Architecture |
| oval:mil.disa.stig.rhel7:def:1375 | [CCE-27471-2] [sshd _disable _empty _passwords] | Disable Empty Passwords |
| oval:mil.disa.stig.rhel7:def:1373 | [CCE-27320-1] [sshd _allow _only _protocol2] | Ensure Only Protocol 2 Connections Allowed |
| oval:mil.disa.stig.rhel7:def:1369 | [CCE-27386-2] [snmpd _not _default _password] | SNMP default communities disabled |

**continues on next page**

**Table 4 – continued from previous page**

| ID | Reference ID | Title |
|---|---|---|
| oval:mil.disa.stig.rhel7:def:1365 | [CCE-27124-7] [set _password _hashing _algorithm _logindefs] | Set SHA512 Password Hashing Algorithm in /etc/login.defs |
| oval:mil.disa.stig.rhel7:def:1229 | [CCE-27286-4] [no _empty _passwords] | The Red Hat Enterprise Linux operating system must not allow accounts configured with blank or null passwords. |
| oval:mil.disa.stig.rhel7:def:120 | [CCE-27311-0] [file _permissions _sshd _pub _key] | SSHD Service Public Key Permissions |
| oval:mil.disa.stig.rhel7:def:1186 | [CCE-80240-5] [mount _option _nosuid _remote _filesystems] | Mount Remote Filesystems with nosuid |
| oval:mil.disa.stig.rhel7:def:118 | [CCE-27485-2] [file _permissions _sshd _private _key] | RHEL-07-040420 - The Red Hat Enterprise Linux operating system must be configured so that the SSH private host key files have mode 0640 or less permissive. |
| oval:mil.disa.stig.rhel7:def:1178 | [CCE-80436-9] [mount _option _noexec _remote _filesystems] | Mount Remote Filesystems with noexec |
| oval:mil.disa.stig.rhel7:def:116 | [CCE-80378-3] [file _owner _cron _allow] | Verify user who owns cron.allow file |
| oval:mil.disa.stig.rhel7:def:114 | [CCE-80379-1] [file _groupowner _cron _allow] | Verify group who owns cron.allow file |
| oval:mil.disa.stig.rhel7:def:1009 | [CCE-80136-5] [dir _perms _world _writable _system _owned] | Find world writable directories not group-owned by a system account |