
Ansible Lockdown RHEL 7 STIG Documentation:

Ansible Lockdown Contributors

Jun 21, 2020

Contents

1	What does the role do?	3
2	Documentation	5
2.1	Getting started	5
2.2	Role Customization	7
2.3	STIG Controls	9
2.4	Additional Controls	409
2.5	Developer Guide	409
2.6	FAQ	410
3	Releases	413
3.1	devel	413

CHAPTER 1

What does the role do?

This role uses the Red Hat Enterprise Linux 7 [Security Technical Implementation Guide \(STIG\)](#) guidance from the [Defense Information Systems Agency \(DISA\)](#). The STIG is released with a public domain license and it is commonly used to secure systems at public and private organizations around the world.

We analyze each configuration hardening item from the applicable STIG benchmark to determine what impact it has on a live production environment and how to best implement it using Ansible. Tasks are added to the role that configure a host to meet the configuration requirements. Each task is documented to explain what was changed, why it was changed, and what deployers need to understand about the change.

Deployers have the option to enable/disable STIG items that do not suit their environments needs. Each STIG item has an associated variable that can be used to switch it on or off. Additionally, the items that have configurable values, i.e. number of password attempts, will generally have a corresponding variable that allows for customization of the applied value. It is imperative for each deployer to understand the regulations and compliance requirements that their organization and specific environments are responsible for meeting in order to effectively implement the controls in the RHEL 7 STIG.

The following documentation applies to the devel branch and is currently under active development. Documentation for the latest stable and previous stable releases will be generated and available once the first stable release is cut.

2.1 Getting started

This role is part of the [Ansible Lockdown](#) project and can be used as a standalone role or it can be used along with other Ansible roles and playbooks.

- *Requirements*
- *Installation*
 - *Using `ansible-galaxy`*
 - *Using `git`*
- *Usage*

2.1.1 Requirements

This documentation assumes that the reader has completed the steps within the [Ansible installation guide](#).

The following additional libraries are required on the Ansible control node:

`passlib` \geq 1.5 (1.6.5 is available in RHEL and CentOS as `python-passlib`)

`jmespath` (available in RHEL and CentOS as `python-jmespath`)

2.1.2 Installation

The recommended installation methods for this role are `ansible-galaxy` (recommended) or `git`.

Using `ansible-galaxy`

The easiest installation method is to use the `ansible-galaxy` command that is provided with your Ansible installation:

```
ansible-galaxy install git+https://github.com/mindpointgroup/rhel7-stig
```

The `ansible-galaxy` command will install the role into `/etc/ansible/roles/rhel7-stig` and this makes it easy to use with Ansible playbooks.

Using `git`

Start by cloning the role into a directory of your choice:

```
mkdir -p ~/.ansible/roles/  
git clone https://github.com/mindpointgroup/rhel7-stig ~/.ansible/roles/rhel7-stig
```

Ansible looks for roles in `~/.ansible/roles` by default.

If the role is cloned into a different directory, that directory must be provided with the `roles_path` option in `ansible.cfg`. The following is an example of a `ansible.cfg` file that uses a custom path for roles:

```
[DEFAULTS]  
roles_path = /etc/ansible/roles:/home/myuser/custom/roles
```

With this configuration, Ansible looks for roles in `/etc/ansible/roles` and `~/custom/roles`.

2.1.3 Usage

This role works well with existing playbooks. The following is an example of a basic playbook that uses this role:

```
---  
- hosts: servers  
  become: yes  
  roles:  
    - role: rhel7-stig  
      when:  
        - ansible_os_family == 'RedHat'  
        - ansible_distribution_major_version | version_compare('7', '=')
```

The role is fully customizable by setting the variables provided in the `defaults/main.yml`. These variables are designed so that categories/severities or individual rules can be enabled, disabled, or can alter configuration for various STIG items in the role. For more details on the available variables, refer to the *STIG Controls* section.

Note: The role requires elevated privileges and must be run as a user with `sudo` access. The example above uses the `become` option, which causes Ansible to use `sudo` before running tasks.

Warning: It is strongly recommended to run the role in check mode (often called a *dry run*) first before making any modifications. This gives the deployer the opportunity to review all of the proposed changes before applying the role to the system. Use the `--check` parameter with `ansible-playbook` to use check mode.

2.2 Role Customization

This role can be fully customized to fit your specific environment. In fact for most users it is recommended that they customize/tweak the role variables before applying across their environment.

- *Tailoring*
 - *Using group_vars*
- *Variables*
 - *Enable tasks by category/severity*
 - *Complex tasks*
 - *Disruptive tasks*
 - *Required system services*
 - *Graphical User Interface items*
 - *Individual STIG rules*

2.2.1 Tailoring

It is recommended that you tailor this roles tasks for your environment by using the comprehensive set of variables defined in `defaults/main.yml`. There are several ways to override default role variables in Ansible. We cover the recommended techniques below.

Using group_vars

The easiest way to tailor this role to your environment is by using `group_vars`:

NEED CONTENT

insert example for group_vars tailoring

2.2.2 Variables

The role has a large number of variables that allow the deployer to control the execution of specific tasks (on/off) as well as the configuration or settings for the tasks and the controls they implement. For example the deployer can choose to enable or disable tasks by severity/category *cat1 | high, cat2 | medium, cat3 | low*. The deployer can also set things like whether any *GUI* related tasks should run or tailor specific STIG settings like the logon banner text or password complexity settings. We don't cover all the variables in this section but we do cover some of the major ones. Generally the variables that control specific tasks or control configurations are detailed in the [controls documentation](#).

Enable tasks by category/severity

These variables allow enabling/disabling cat1, cat2, or cat3 rules in bulk. Disabling these will take precedence over individual task variables but enabling them will not. i.e. If the `rhel7stig_cat3_patch` variable is set to `no` then all `cat3` tasks will be skipped regardless of their *individual settings*. However if the `cat3` variable is enabled individual tasks could still be skipped if their variable is disabled.

```
rhel7stig_cat1_patch: yes
rhel7stig_cat2_patch: yes
rhel7stig_cat3_patch: yes
```

Complex tasks

There are several variables that control the execution or behavior of tasks that the implementers of this role have deemed to be too complex or risky to automatically remediate. These rules have tasks that audit the system and will optionally report changed and will report back (via debug statements) if the system would fail the check. The deployer can use this information to manually remediate the finding. The execution and reporting behavior of these tasks is controlled by two variables:

```
# Controls execution of these tasks
rhel7stig_complexity_high: no

# Controls whether the tasks reports changed or not
rhel7stig_audit_complex: yes
```

Disruptive tasks

These variables are similar to the *complex task* variables. They control the execution or behavior of tasks that perform automated remediation but are shown to be potentially disruptive to systems when used in production environments. The risk of automated remediation of with these tasks is high. These rules have tasks that audit the system and will optionally report changed and will report back (via debug statements) if the system would fail the check. The deployer can use this information to manually remediate the finding. The execution and reporting behavior of these tasks is controlled by two variables:

```
# Controls execution of these tasks
rhel7stig_disruption_high: no

# Controls whether the tasks reports changed or not
rhel7stig_audit_disruptive: yes
```

Required system services

These variables allow the deployer to specify that services are required by the system to perform its mission. Except for `ssh`, it is important to note that having these services installed and enabled are deviations from the STIG benchmark and should have corresponding documentation approved by the system owner or other signing authority.

```
rhel7stig_ssh_required: yes
rhel7stig_vsftpd_required: no
rhel7stig_tftp_required: no
rhel7stig_autofs_required: no
rhel7stig_kdump_required: no
rhel7stig_ipsec_required: no
```

Graphical User Interface items

This variable enables or disables all tasks related to *GUI* packages. i.e. These generally would only apply to a system with the *GNOME* package installed. This is not to say that *KDE*, *XFCE*, or one of the many other desktop systems would not need to have similar controls in place, but the STIG currently only covers *GNOME* settings.

```
rhel7stig_gui: no
```

Individual STIG rules

These variables enable or disable individual rules or more specifically tasks or blocks of tasks that enforce individual STIG rules. Each STIG item with an ID following the format *RHEL-07-#####* (ex. *RHEL-07-010010*) will have a corresponding variable in the below format. For more information on each rule and its default state please see the *controls documentation*.

```
rhel_07_#####: true
```

2.3 STIG Controls

This role follows the Red Hat Enterprise Linux 7 [Security Technical Implementation Guide \(STIG\)](#). The guide has over 200 controls that apply to various parts of a Linux system, and it is updated regularly by the Defense Information Systems Agency (DISA). DISA is part of the United States Department of Defense. The current version of this role follows Version 2, Release 1 of the RHEL 7 STIG.

Controls are divided into groups based on the following properties:

2.3.1 Control Severities

High (CAT I) These controls have a large impact on the security of a system. They also have the largest operational impact to a system and deployers should test them thoroughly in non-production environments.

Medium (CAT II) These controls are the bulk of the items in the STIG and they have a moderate level of impact on the security of a system. Many controls in this category will have an operational impact on a system and should be tested thoroughly before implementation.

Low (CAT III) These controls have a smaller impact on overall security, but they are generally easier to implement with a much lower operational impact.

2.3.2 Implementation Status

It is important to understand the implementation status of each control and the potential impact each task can have on a system. Some controls are not implemented for various technical reasons. Some are implemented but disabled by default. And others are just perform a check and report back if manual changes need to be made to meet the STIG control.

Implemented These controls are fully implemented and they may have configurations which can be adjusted. The notes for each control will identify which configuration options are available.

Complexity High These controls are deemed too complex to safely remediate via automated controls. The tasks for these controls perform automated checks and will report the result of the check in Ansible task output. The purpose of this output is to alert deployers to items that would fail an audit against the STIG and should be

remediated manually. Execution and reporting from these tasks can be enabled or disabled via the appropriate variables.

```
rhel7stig_complexity_high: no
rhel7stig_audit_complex: yes
```

Disruption High These controls are classified as having a high likelihood of disruption on a system and disabled by default. Automatic remediation can be enabled by setting the appropriate variables, however the deployer should be aware that they are often disabled because they could cause harm to a subset of systems. Each control has notes that explains the caveats of the control and how to enable it if needed.

```
rhel7stig_disruption_high: no
rhel7stig_audit_disruptive: yes
```

Not Implemented These are controls that have not yet been implemented. The goal of this project is to have no controls in this status. This does not mean 100% of the controls will be fully implemented. Just that 100% of the controls will be in one of the above status categories. We welcome any help in getting these controls implemented.

Deployers should review the full list of controls *sorted by implementation status*.

2.3.3 Control Deviation

The role deviates from some of the STIG's requirements when a security control could cause significant issues with production systems. Additionally specific control settings, which are controlled by role variables, can deviate from the mandated STIG settings. Deployers should review and update the default configurations to meet the needs of their environment.

Note: All of the default configurations are found within `defaults/main.yml`.

2.3.4 Controls

All Controls

Navigating the list

Use your browser's search function (usually CTRL-f or -f) to find the security configuration in the full list shown here. You can search for STIG ID numbers, such as RHEL-07-010010, Vulnerability ID numbers, such as V-38463, or for implementation statuses, like Not Implemented.

RHEL-07-010010 (V-71849)

The Red Hat Enterprise Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.

Severity: High

Implementation Status: Implemented

Description:

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Variables:

rhel_07_010010

Tags:

RHEL-07-010010

Notes:

Nothing to report

RHEL-07-010020 (V-71855)

The Red Hat Enterprise Linux operating system must be configured so that the cryptographic hash of system files and commands matches vendor values.

Severity: High

Implementation Status: Implemented

Description:

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_010020

Tags:

RHEL-07-010020

Notes:

Nothing to report

RHEL-07-010030 (V-71859)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

```
rhel7stig_dconf_available
rhel_07_010030
rhel_07_010040
```

Tags:

```
RHEL-07-010030
RHEL_07_010040
dod_logon_banner
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010040 (V-71861)

The Red Hat Enterprise Linux operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

Severity: Medium

Implementation Status: Not Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

Tags:**Notes:**

Nothing to report

RHEL-07-010050 (V-71863)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
```

(continues on next page)

(continued from previous page)

the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Variables:

```
rhel_07_010050
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010050
ssh
dod_logon_banner
```

Notes:

Nothing to report

RHEL-07-010060 (V-71891)

The Red Hat Enterprise Linux operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures.

Severity: Medium

Implementation Status: Implemented

Description:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Variables:

```
rhel7stig_dconf_available
rhel_07_010060
```

Tags:

```
RHEL-07-010060
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010061 (V-77819)

The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.

Severity: Medium

Implementation Status: Implemented

Description:

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Variables:

```
rhel7stig_dconf_available  
rhel_07_010061
```

Tags:

```
RHEL-07-010061  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010070 (V-71893)

The Red Hat Enterprise Linux operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010070
```

Tags:

```
RHEL-07-010070  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010081 (V-73155)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver lock-delay setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010081
```

Tags:

```
RHEL-07-010081  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010082 (V-73157)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010082
```

Tags:

```
RHEL-07-010082  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010090 (V-71897)

The Red Hat Enterprise Linux operating system must have the screen package installed.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The screen package allows for a session lock to be implemented and configured.

Variables:

```
rhel_07_010090
```

Tags:

```
RHEL-07-010090
```

Notes:

Nothing to report

RHEL-07-010100 (V-71899)

The Red Hat Enterprise Linux operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available
rhel_07_010100
```

Tags:

```
RHEL-07-010100
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010101 (V-78997)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Variables:

```
rhel7stig_dconf_available
rhel_07_010101
```

Tags:

```
RHEL-07-010101
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010110 (V-71901)

The Red Hat Enterprise Linux operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available
rhel_07_010110
```

Tags:

```
RHEL-07-010110
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010118 (V-81003)

The Red Hat Enterprise Linux operating system must be configured so that /etc/pam.d/passwd implements /etc/pam.d/system-auth when changing passwords.

Severity: Medium

Implementation Status: Not Implemented

Description:

Pluggable authentication modules (PAM) allow for a modular approach to integrating authentication methods. PAM operates in a top-down processing model and if the modules are not listed in the correct order, an important security function could be bypassed if stack entries are not centralized.

Variables:**Tags:****Notes:**

Nothing to report

RHEL-07-010119 (V-73159)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. “pwquality” enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

Variables:

rhel_07_010119

Tags:

RHEL-07-010119
pamd

Notes:

Nothing to report

RHEL-07-010120 (V-71903)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one upper-case character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010120
```

Tags:

```
RHEL-07-010120  
pwquality
```

Notes:

Nothing to report

RHEL-07-010130 (V-71905)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one lower-case character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010130
```

Tags:

```
RHEL-07-010130  
pwquality
```

Notes:

Nothing to report

RHEL-07-010140 (V-71907)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010140
```

Tags:

```
RHEL-07-010140  
pwquality
```

Notes:

Nothing to report

RHEL-07-010150 (V-71909)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one special character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010150
```

Tags:

```
RHEL-07-010150  
pwquality
```

Notes:

Nothing to report

RHEL-07-010160 (V-71911)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of eight of the total number of characters must be changed.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010160
```

Tags:

```
RHEL-07-010160  
pwquality
```

Notes:

Nothing to report

RHEL-07-010170 (V-71913)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of four character classes must be changed.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010170
```

Tags:

RHEL-07-010170 pwquality

Notes:

Nothing to report

RHEL-07-010180 (V-71915)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed the number of repeating consecutive characters must not be more than three characters.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

rhel_07_010180

Tags:

RHEL-07-010180 pwquality

Notes:

Nothing to report

RHEL-07-010190 (V-71917)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010190
```

Tags:

```
RHEL-07-010190  
pwquality
```

Notes:

Nothing to report

RHEL-07-010200 (V-71919)

The Red Hat Enterprise Linux operating system must be configured so that the PAM system service is configured to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

```
rhel_07_010200
```

Tags:

```
RHEL-07-010200  
pamd
```

Notes:

Nothing to report

RHEL-07-010210 (V-71921)

The Red Hat Enterprise Linux operating system must be configured to use the shadow file to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

rhel_07_010210

Tags:

RHEL-07-010210
login

Notes:

Nothing to report

RHEL-07-010220 (V-71923)

The Red Hat Enterprise Linux operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

rhel_07_010220

Tags:

RHEL-07-010220

Notes:

Nothing to report

RHEL-07-010230 (V-71925)

The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 24 hours/1 day minimum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Variables:

```
rhel_07_010230
```

Tags:

```
RHEL-07-010230  
login
```

Notes:

Nothing to report

RHEL-07-010240 (V-71927)

The Red Hat Enterprise Linux operating system must be configured so that passwords are restricted to a 24 hours/1 day minimum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Variables:

```
rhel_07_010240
```

Tags:

```
RHEL-07-010240  
password
```

Notes:

Nothing to report

RHEL-07-010250 (V-71929)

The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 60-day maximum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Variables:

```
rhel_07_010250
```

Tags:

```
RHEL-07-010250  
login
```

Notes:

Nothing to report

RHEL-07-010260 (V-71931)

The Red Hat Enterprise Linux operating system must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

Severity: Medium

Implementation Status: Disruption High

Description:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Variables:

```
rhel_07_010260  
rhel7stig_disruptive
```

Tags:

```
RHEL-07-010260  
disruption-high  
password
```

Notes:

Nothing to report

RHEL-07-010270 (V-71933)

The Red Hat Enterprise Linux operating system must be configured so that passwords are prohibited from reuse for a minimum of five generations.

Severity: Medium

Implementation Status: Implemented

Description:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Variables:

```
rhel_07_010270
```

Tags:

```
RHEL-07-010270  
pamd
```

Notes:

Nothing to report

RHEL-07-010280 (V-71935)

The Red Hat Enterprise Linux operating system must be configured so that passwords are a minimum of 15 characters in length.

Severity: Medium

Implementation Status: Implemented

Description:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Variables:

```
rhel_07_010280
```

Tags:

```
RHEL-07-010280  
pwquality
```

Notes:

Nothing to report

RHEL-07-010290 (V-71937)

The Red Hat Enterprise Linux operating system must not have accounts configured with blank or null passwords.

Severity: High

Implementation Status: Implemented

Description:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Variables:

```
rhel_07_010290
```

Tags:

```
RHEL-07-010290  
pamd
```

Notes:

Nothing to report

RHEL-07-010300 (V-71939)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using an empty password.

Severity: High

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_010300  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010300  
ssh
```

Notes:

Nothing to report

RHEL-07-010310 (V-71941)

The Red Hat Enterprise Linux operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

Severity: Medium

Implementation Status: Implemented

Description:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Variables:

```
rhel_07_010310
```

Tags:

```
RHEL-07-010310
```

Notes:

Nothing to report

RHEL-07-010320 (V-71943)

Accounts on the Red Hat Enterprise Linux operating system that are subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period.

Severity: Medium

Implementation Status: Implemented

Description:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Variables:

```
rhel_07_010320 or rhel_07_010330
```

Tags:

```
RHEL-07-010320  
RHEL-07-010330  
pamd
```

Notes:

Nothing to report

RHEL-07-010330 (V-71945)

The Red Hat Enterprise Linux operating system must lock the associated account after three unsuccessful root logon attempts are made within a 15-minute period.

Severity: Medium

Implementation Status: Implemented

Description:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Variables:

```
rhel_07_010320 or rhel_07_010330
```

Tags:

```
RHEL-07-010320  
RHEL-07-010330  
pamd
```

Notes:

Nothing to report

RHEL-07-010340 (V-71947)

The Red Hat Enterprise Linux operating system must be configured so that users must provide a password for privilege escalation.

Severity: Medium

Implementation Status: Implemented

Description:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Variables:

```
rhel7stig_using_password_auth  
rhel_07_010340
```

Tags:

```
RHEL-07-010340  
sudoers
```

Notes:

Nothing to report

RHEL-07-010350 (V-71949)

The Red Hat Enterprise Linux operating system must be configured so that users must re-authenticate for privilege escalation.

Severity: Medium

Implementation Status: Implemented

Description:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Variables:

```
rhel_07_010350
```

Tags:

```
RHEL-07-010350  
sudoers
```

Notes:

Nothing to report

RHEL-07-010430 (V-71951)

The Red Hat Enterprise Linux operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Variables:

`rhel_07_010430`

Tags:

`RHEL-07-010430`
`login`

Notes:

Nothing to report

RHEL-07-010440 (V-71953)

The Red Hat Enterprise Linux operating system must not allow an unattended or automatic logon to the system via a graphical user interface.

Severity: High

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

`rhel7stig_gui`
`rhel_07_010440`

Tags:

`RHEL-07-010440`
`gui`

Notes:

Nothing to report

RHEL-07-010450 (V-71955)

The Red Hat Enterprise Linux operating system must not allow an unrestricted logon to the system.

Severity: High

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

`rhel7stig_gui`
`rhel_07_010450`

Tags:

```
RHEL-07-010450  
gui
```

Notes:

Nothing to report

RHEL-07-010460 (V-71957)

The Red Hat Enterprise Linux operating system must not allow users to override SSH environment variables.

Severity: Medium

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel_07_010460  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010460  
ssh
```

Notes:

Nothing to report

RHEL-07-010470 (V-71959)

The Red Hat Enterprise Linux operating system must not allow a non-certificate trusted host SSH logon to the system.

Severity: Medium

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010470  
ssh
```


Notes:

Nothing to report

RHEL-07-010480 (V-71961)

Red Hat Enterprise Linux operating systems prior to version 7.2 with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010480 or rhel_07_010490
ansible_distribution_version is version_compare('7.2', '<')
```

Tags:

```
RHEL-07-010480
RHEL-07-010490
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010481 (V-77823)

The Red Hat Enterprise Linux operating system must require authentication upon booting into single-user and maintenance modes.

Severity: Medium

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Variables:

```
rhel_07_010481
```

Tags:

```
RHEL-07-010481
rescue
```

Notes:

Nothing to report

RHEL-07-010482 (V-81005)

Red Hat Enterprise Linux operating systems version 7.2 or newer with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010482 or rhel_07_010491
ansible_distribution_version is version_compare('7.2', '>=')
```

Tags:

```
RHEL-07-010482
RHEL-07-010491
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010490 (V-71963)

Red Hat Enterprise Linux operating systems prior to version 7.2 using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010480 or rhel_07_010490
ansible_distribution_version is version_compare('7.2', '<')
```

Tags:

```
RHEL-07-010480
RHEL-07-010490
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010491 (V-81007)

Red Hat Enterprise Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010482 or rhel_07_010491
ansible_distribution_version is version_compare('7.2', '>=')
```

Tags:

```
RHEL-07-010482
RHEL-07-010491
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010500 (V-71965)

The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.

Severity: Medium

Implementation Status: Not Implemented

Description:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

- 1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication;

and

- 2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Variables:

```
rhel_07_010500
```

Tags:

```
RHEL-07-010500  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020000 (V-71967)

The Red Hat Enterprise Linux operating system must not have the rsh-server package installed.

Severity: High

Implementation Status: Implemented

Description:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Variables:

`rhel_07_020000`

Tags:

`RHEL-07-020000`
`rsh`

Notes:

Nothing to report

RHEL-07-020010 (V-71969)

The Red Hat Enterprise Linux operating system must not have the ypserv package installed.

Severity: High

Implementation Status: Implemented

Description:

Removing the “ypserv” package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Variables:

`rhel_07_020010`

Tags:

`RHEL-07-020010`
`ypserv`

Notes:

Nothing to report

RHEL-07-020020 (V-71971)

The Red Hat Enterprise Linux operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Severity: Medium

Implementation Status: Not Implemented

Description:

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Variables:

```
rhel_07_020020
```

Tags:

```
RHEL-07-020020  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020030 (V-71973)

The Red Hat Enterprise Linux operating system must be configured so that a file integrity tool verifies the baseline operating system configuration at least weekly.

Severity: Medium

Implementation Status: Implemented

Description:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Variables:

```
rhel_07_020030 or rhel_07_020040
```

Tags:

```
RHEL-07-020030  
RHEL-07-020040  
aide
```

Notes:

Nothing to report

RHEL-07-020040 (V-71975)

The Red Hat Enterprise Linux operating system must be configured so that designated personnel are notified if baseline configurations are changed in an unauthorized manner.

Severity: Medium

Implementation Status: Implemented

Description:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Variables:

```
rhel_07_020030 or rhel_07_020040
```

Tags:

```
RHEL-07-020030  
RHEL-07-020040  
aide
```

Notes:

Nothing to report

RHEL-07-020050 (V-71977)

The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Severity: High

Implementation Status: Implemented

Description:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Variables:

```
rhel_07_020050
```

Tags:

```
RHEL-07-020050  
yum
```

Notes:

Nothing to report

RHEL-07-020060 (V-71979)

The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Severity: High

Implementation Status: Implemented

Description:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Variables:

```
rhel_07_020060
```

Tags:

```
RHEL-07-020060  
yum
```

Notes:

Nothing to report

RHEL-07-020100 (V-71983)

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

Severity: Medium

Implementation Status: Implemented

Description:

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Variables:

rhel_07_020100

Tags:

RHEL-07-020100
usb_devices

Notes:

Nothing to report

RHEL-07-020101 (V-77821)

The Red Hat Enterprise Linux operating system must be configured so that the Datagram Congestion Control Protocol (DCCP) kernel module is disabled unless required.

Severity: Medium

Implementation Status: Implemented

Description:

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Variables:

rhel_07_020101

Tags:

RHEL-07-020101
dccp

Notes:

Nothing to report

RHEL-07-020110 (V-71985)

The Red Hat Enterprise Linux operating system must disable the file system automounter unless required.

Severity: Medium

Implementation Status: Implemented

Description:

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_020110
rhel_07_020110
rhel_07_020110_autofs_service_status.stdout == "loaded"
not rhel7stig_autofs_required
```

Tags:

```
RHEL-07-020110
```

Notes:

Nothing to report

RHEL-07-020200 (V-71987)

The Red Hat Enterprise Linux operating system must remove all software components after updated versions have been installed.

Severity: Low

Implementation Status: Implemented

Description:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Variables:

```
rhel_07_020200
```

Tags:

```
RHEL-07-020200
```

Notes:

Nothing to report

RHEL-07-020210 (V-71989)

The Red Hat Enterprise Linux operating system must enable SELinux.

Severity: High

Implementation Status: Implemented

Description:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Variables:

```
rhel_07_020210 or rhel_07_020220  
not rhel7stig_system_is_container
```

Tags:

```
RHEL-07-020210  
RHEL-07-020220  
selinux
```

Notes:

Nothing to report

RHEL-07-020220 (V-71991)

The Red Hat Enterprise Linux operating system must enable the SELinux targeted policy.

Severity: High

Implementation Status: Implemented

Description:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Variables:

```
rhel_07_020210 or rhel_07_020220  
not rhel7stig_system_is_container
```

Tags:

```
RHEL-07-020210  
RHEL-07-020220  
selinux
```

Notes:

Nothing to report

RHEL-07-020230 (V-71993)

The Red Hat Enterprise Linux operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled.

Severity: High

Implementation Status: Implemented

Description:

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Variables:

rhel_07_020230

Tags:

RHEL-07-020230

Notes:

Nothing to report

RHEL-07-020240 (V-71995)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Variables:

rhel_07_020240

Tags:

RHEL-07-020240
login
umask

Notes:

Nothing to report

RHEL-07-020250 (V-71997)

The Red Hat Enterprise Linux operating system must be a vendor supported release.

Severity: High

Implementation Status: Complexity High

Description:

An operating system release is considered “supported” if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Variables:

```
rhel_07_020250
rhel7stig_complex
```

Tags:

```
RHEL-07-020250
complexity-high
```

Notes:

Nothing to report

RHEL-07-020260 (V-71999)

The Red Hat Enterprise Linux operating system security patches and updates must be installed and up to date.

Severity: Medium

Implementation Status: Implemented

Description:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Variables:

```
rhel_07_020260
rhel_07_020260
rhel_07_020260
rhel7stig_auto_package_updates_enabled or rhel_07_020260_yum_cron_installed.rc == 0
```

Tags:

```
RHEL-07-020260
packaging
```

Notes:

Nothing to report

RHEL-07-020270 (V-72001)

The Red Hat Enterprise Linux operating system must not have unnecessary accounts.

Severity: Medium

Implementation Status: Implemented

Description:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Variables:

```
rhel_07_020270
```

Tags:

```
RHEL-07-020270
```

Notes:

Nothing to report

RHEL-07-020300 (V-72003)

The Red Hat Enterprise Linux operating system must be configured so that all Group Identifiers (GIDs) referenced in the /etc/passwd file are defined in the /etc/group file.

Severity: Low

Implementation Status: Complexity High

Description:

If a user is assigned the GID of a group not existing on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Variables:

```
rhel_07_020300  
rhel7stig_complex
```

Tags:

```
RHEL-07-020300  
complexity-high  
passwd
```

Notes:

Nothing to report

RHEL-07-020310 (V-72005)

The Red Hat Enterprise Linux operating system must be configured so that the root account must be the only account having unrestricted access to the system.

Severity: High

Implementation Status: Implemented

Description:

If an account other than root also has a User Identifier (UID) of “0”, it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of “0” afford an opportunity for potential intruders to guess a password for a privileged account.

Variables:

```
rhel_07_020310
```

Tags:

```
RHEL-07-020310
```

Notes:

Nothing to report

RHEL-07-020320 (V-72007)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid owner.

Severity: Medium

Implementation Status: Complexity High

Description:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier “UID” as the UID of the un-owned files.

Variables:

```
rhel_07_020320  
rhel7stig_complex
```

Tags:

```
RHEL-07-020320  
complexity-high
```

Notes:

Nothing to report

RHEL-07-020330 (V-72009)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid group owner.

Severity: Medium

Implementation Status: Complexity High

Description:

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Variables:

```
rhel_07_020330  
rhel7stig_complex
```

Tags:

```
RHEL-07-020330  
complexity-high
```

Notes:

Nothing to report

RHEL-07-020600 (V-72011)

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.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Variables:

```
rhel_07_020600
```

Tags:

```
RHEL-07-020600
```


Notes:

Nothing to report

RHEL-07-020610 (V-72013)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Variables:

```
rhel_07_020610
```

Tags:

```
RHEL-07-020610  
login  
home
```

Notes:

Nothing to report

RHEL-07-020620 (V-72015)

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.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the / directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Variables:

```
rhel_07_020620  
item.uid >= 1000  
item.uid != 65534
```

Tags:

RHEL-07-020620

Notes:

Nothing to report

RHEL-07-020630 (V-72017)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories have mode 0750 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Variables:

```
rhel_07_020630
item.uid >= 1000
item.uid != 65534
```

Tags:

RHEL-07-020630

Notes:

Nothing to report

RHEL-07-020640 (V-72019)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are owned by their respective users.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user does not own their home directory, unauthorized users could access or modify the user's files, and the users may not be able to access their own files.

Variables:

```
rhel_07_020640
item.uid >= 1000
item.uid != 65534
```

Tags:

RHEL-07-020640

Notes:

Nothing to report

RHEL-07-020650 (V-72021)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners primary group.

Severity: Medium

Implementation Status: Implemented

Description:

If the Group Identifier (GID) of a local interactive user's home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

Variables:

```
rhel_07_020650
item.uid >= 1000
item.uid != 65534
```

Tags:

RHEL-07-020650

Notes:

Nothing to report

RHEL-07-020660 (V-72023)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are owned by the owner of the home directory.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Variables:

rhel_07_020660

Tags:

RHEL-07-020660

Notes:

Nothing to report

RHEL-07-020670 (V-72025)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Variables:

rhel_07_020670

Tags:

RHEL-07-020670

Notes:

Nothing to report

RHEL-07-020680 (V-72027)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Variables:

rhel_07_020680

Tags:

RHEL-07-020680

Notes:

Nothing to report

RHEL-07-020690 (V-72029)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for interactive users are owned by the home directory user or root.

Severity: Medium

Implementation Status: Implemented

Description:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020690

Tags:

RHEL-07-020690

Notes:

Nothing to report

RHEL-07-020700 (V-72031)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for local interactive users are be group-owned by the users primary group or root.

Severity: Medium

Implementation Status: Implemented

Description:

Local initialization files for interactive users are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020700

Tags:

RHEL-07-020700

Notes:

Nothing to report

RHEL-07-020710 (V-72033)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files have mode 0740 or less permissive.

Severity: Medium

Implementation Status: Not Implemented

Description:

Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon login.

Variables:

```
rhel_07_020710
```

Tags:

```
RHEL-07-020710  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020720 (V-72035)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user initialization files executable search paths contain only paths that resolve to the users home directory.

Severity: Medium

Implementation Status: Not Implemented

Description:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Variables:

```
rhel_07_020720
```

Tags:

```
RHEL-07-020720  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020730 (V-72037)

The Red Hat Enterprise Linux operating system must be configured so that local initialization files do not execute world-writable programs.

Severity: Medium

Implementation Status: Not Implemented

Description:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Variables:

```
rhel_07_020730
```

Tags:

```
RHEL-07-020730  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020900 (V-72039)

The Red Hat Enterprise Linux operating system must be configured so that all system device files are correctly labeled to prevent unauthorized modification.

Severity: Medium

Implementation Status: Complexity High

Description:

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Variables:

```
rhel_07_020900  
rhel7stig_complex  
ansible_selinux is not defined  
rhel_07_020900  
rhel7stig_complex  
ansible_selinux.status == "enabled"
```

Tags:

```
RHEL-07-020900  
complexity-high
```

Notes:

Nothing to report

RHEL-07-021000 (V-72041)

The Red Hat Enterprise Linux operating system must be configured so that file systems containing user home directories are mounted to prevent files with the setuid and setgid bit set from being executed.

Severity: Medium

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setgid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021000
ansible_mounts | selectattr('mount', 'match', '^/home$') | list | length != 0
'nosuid' not in home_mount.options
```

Tags:

```
RHEL-07-021000
```

Notes:

Nothing to report

RHEL-07-021010 (V-72043)

The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are used with removable media.

Severity: Medium

Implementation Status: Not Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021010
```

Tags:


```
RHEL-07-021010  
notimplemented
```

Notes:

Nothing to report

RHEL-07-021020 (V-72045)

The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are being imported via Network File System (NFS).

Severity: Medium

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021020  
'nosuid' not in (ansible_mounts | json_query(options_query))
```

Tags:

```
RHEL-07-021020
```

Notes:

Nothing to report

RHEL-07-021021 (V-73161)

The Red Hat Enterprise Linux operating system must prevent binary files from being executed on file systems that are being imported via Network File System (NFS).

Severity: Medium

Implementation Status: Implemented

Description:

The “noexec” mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021021  
'noexec' not in (ansible_mounts | json_query(options_query))
```

Tags:

RHEL-07-021021

Notes:

Nothing to report

RHEL-07-021022 (V-81009)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the nodev option.

Severity: Low

Implementation Status: Implemented

Description:

The “nodev” mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

rhel_07_021022 or rhel_07_021023 or rhel_07_021024

Tags:

RHEL-07-021022
RHEL-07-021023
RHEL-07-021024

Notes:

Nothing to report

RHEL-07-021023 (V-81011)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the nosuid option.

Severity: Low

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

rhel_07_021022 or rhel_07_021023 or rhel_07_021024

Tags:

RHEL-07-021022
RHEL-07-021023
RHEL-07-021024

Notes:

Nothing to report

RHEL-07-021024 (V-81013)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the noexec option.

Severity: Low

Implementation Status: Implemented

Description:

The “noexec” mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

rhel_07_021022 or rhel_07_021023 or rhel_07_021024

Tags:

RHEL-07-021022
RHEL-07-021023
RHEL-07-021024

Notes:

Nothing to report

RHEL-07-021030 (V-72047)

The Red Hat Enterprise Linux operating system must be configured so that all world-writable directories are group-owned by root, sys, bin, or an application group.

Severity: Medium

Implementation Status: Disruption High

Description:

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Variables:

```
rhel_07_021030
rhel7stig_disruptive
```

Tags:

```
RHEL-07-021030
disruption-high
```

Notes:

Nothing to report

RHEL-07-021040 (V-72049)

The Red Hat Enterprise Linux operating system must set the umask value to 077 for all local interactive user accounts.

Severity: Medium

Implementation Status: Not Implemented

Description:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be “0”. This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Variables:

```
rhel_07_021040
```

Tags:

```
RHEL-07-021040
notimplemented
```

Notes:

Nothing to report

RHEL-07-021100 (V-72051)

The Red Hat Enterprise Linux operating system must have cron logging implemented.

Severity: Medium

Implementation Status: Implemented

Description:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Variables:

`rhel_07_021100`

Tags:

`RHEL-07-021100`

Notes:

Nothing to report

RHEL-07-021110 (V-72053)

The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is owned by root.

Severity: Medium

Implementation Status: Implemented

Description:

If the owner of the “cron.allow” file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Variables:

`rhel_07_021110`
`rhel_07_021120`

Tags:

`RHEL-07-021110`
`RHEL-07-021120`
`cron`

Notes:

Nothing to report

RHEL-07-021120 (V-72055)

The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is group-owned by root.

Severity: Medium

Implementation Status: Implemented

Description:

If the group owner of the “cron.allow” file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Variables:

```
rhel_07_021110  
rhel_07_021120
```

Tags:

```
RHEL-07-021110  
RHEL-07-021120  
cron
```

Notes:

Nothing to report

RHEL-07-021300 (V-72057)

The Red Hat Enterprise Linux operating system must disable Kernel core dumps unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Variables:

```
rhel_07_021300
```

Tags:

```
RHEL-07-021300
```

Notes:

Nothing to report

RHEL-07-021310 (V-72059)

The Red Hat Enterprise Linux operating system must be configured so that a separate file system is used for user home directories (such as /home or an equivalent).

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021310
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/home$') | list | length == 0
```

Tags:

```
RHEL-07-021310
complexity-high
mount
home
```

Notes:

Nothing to report

RHEL-07-021320 (V-72061)

The Red Hat Enterprise Linux operating system must use a separate file system for /var.

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021320
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/var$') | list | length == 0
```

Tags:

```
RHEL-07-021320
complexity-high
mount
var
```

Notes:

Nothing to report

RHEL-07-021330 (V-72063)

The Red Hat Enterprise Linux operating system must use a separate file system for the system audit data path.

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021330
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/var/log/audit$') | list | length == 0
```

Tags:

```
RHEL-07-021330
complexity-high
mount
auditd
```

Notes:

Nothing to report

RHEL-07-021340 (V-72065)

The Red Hat Enterprise Linux operating system must use a separate file system for /tmp (or equivalent).

Severity: Low

Implementation Status: Implemented

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
rhel_07_021340
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
ansible_mounts | selectattr('mount', 'match', '^/tmp$') | list | length == 0
```

Tags:

```
RHEL-07-021340
mount
tmp
```

Notes:

Nothing to report

RHEL-07-021350 (V-72067)

The Red Hat Enterprise Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Severity: High

Implementation Status: Implemented

Description:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Variables:

```
rhel_07_021350
ansible_distribution_major_version == '7'
```

Tags:

```
RHEL-07-021350
```

Notes:

Nothing to report

RHEL-07-021600 (V-72069)

The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).

Severity: Low

Implementation Status: Not Implemented

Description:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Variables:

```
rhel_07_021600
```

Tags:

```
RHEL-07-021600
notimplemented
```

Notes:

Nothing to report

RHEL-07-021610 (V-72071)

The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify extended attributes.

Severity: Low

Implementation Status: Not Implemented

Description:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Variables:

```
rhel_07_021610
```

Tags:

```
RHEL-07-021610  
notimplemented
```

Notes:

Nothing to report

RHEL-07-021620 (V-72073)

The Red Hat Enterprise Linux operating system must use a file integrity tool that is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Severity: Medium

Implementation Status: Implemented

Description:

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Variables:

```
rhel_07_021620
```

Tags:

```
aide  
RHEL-07-021620
```

Notes:

Nothing to report

RHEL-07-021700 (V-72075)

The Red Hat Enterprise Linux operating system must not allow removable media to be used as the boot loader unless approved.

Severity: Medium

Implementation Status: Not Implemented

Description:

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Variables:

```
rhel_07_021700
```

Tags:

```
RHEL-07-021700  
notimplemented
```

Notes:

Nothing to report

RHEL-07-021710 (V-72077)

The Red Hat Enterprise Linux operating system must not have the telnet-server package installed.

Severity: High

Implementation Status: Implemented

Description:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Variables:

```
rhel_07_021710
```

Tags:

```
RHEL-07-021710  
telnet
```

Notes:

Nothing to report

RHEL-07-030000 (V-72079)

The Red Hat Enterprise Linux operating system must be configured so that auditing is configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.

Severity: High

Implementation Status: Implemented

Description:

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096

Variables:

```
rhel_07_030000
```

Tags:

```
RHEL-07-030000  
auditd
```

Notes:

Nothing to report

RHEL-07-030010 (V-72081)

The Red Hat Enterprise Linux operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.

Severity: Medium

Implementation Status: Implemented

Description:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Variables:

`rhel_07_030010`

Tags:

`auditd`
`RHEL-07-030010`

Notes:

Nothing to report

RHEL-07-030200 (V-81015)

The Red Hat Enterprise Linux operating system must be configured to use the au-remote plugin.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the “au-remote” plugin, the audisp-remote daemon will not off-load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

`rhel_07_030200`

Tags:

`auditd`
`RHEL-07-030200`

Notes:

Nothing to report

RHEL-07-030201 (V-81017)

The Red Hat Enterprise Linux operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the “au-remote” plugin, the audisp-remote daemon will not off load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030210 (V-81019)

The Red Hat Enterprise Linux operating system must take appropriate action when the audisp-remote buffer is full.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When the remote buffer is full, audit logs will not be collected and sent to the central log server.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030211 (V-81021)

The Red Hat Enterprise Linux operating system must label all off-loaded audit logs before sending them to the central log server.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:**Tags:****Notes:**

Nothing to report

RHEL-07-030300 (V-72083)

The Red Hat Enterprise Linux operating system must off-load audit records onto a different system or media from the system being audited.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

rhel_07_030300 and rhel7stig_audisp_remote_server

Tags:

```
auditd  
RHEL-07-030300
```

Notes:

Nothing to report

RHEL-07-030310 (V-72085)

The Red Hat Enterprise Linux operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

```
rhel_07_030310
```

Tags:

```
auditd  
RHEL-07-030310
```

Notes:

Nothing to report

RHEL-07-030320 (V-72087)

The Red Hat Enterprise Linux operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.

Severity: Medium

Implementation Status: Implemented

Description:

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Variables:

```
rhel_07_030320
```

Tags:

`auditd`
`RHEL-07-030320`

Notes:

Nothing to report

RHEL-07-030321 (V-73163)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Variables:

`rhel_07_030321`

Tags:

`auditd`
`RHEL-07-030321`

Notes:

Nothing to report

RHEL-07-030330 (V-72089)

The Red Hat Enterprise Linux operating system must initiate an action to notify the System Administrator (SA) and Information System Security Officer ISSO, at a minimum, when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Variables:

`rhel_07_030330`

Tags:

```
auditd  
RHEL-07-030330
```

Notes:

Nothing to report

RHEL-07-030340 (V-72091)

The Red Hat Enterprise Linux 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.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Variables:

```
rhel_07_030340
```

Tags:

```
auditd  
RHEL-07-030340
```

Notes:

Nothing to report

RHEL-07-030350 (V-72093)

The Red Hat Enterprise Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Variables:

```
rhel_07_030350
```

Tags:

```
auditd
RHEL-07-030350
```

Notes:

Nothing to report

RHEL-07-030360 (V-72095)

The Red Hat Enterprise Linux operating system must audit all executions of privileged functions.

Severity: Medium

Implementation Status: Implemented

Description:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Variables:

```
rhel_07_030360
```

Tags:

```
audit-rules
RHEL-07-030360
```

Notes:

Nothing to report

RHEL-07-030370 (V-72097)

The Red Hat Enterprise Linux operating system must audit all uses of the chown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030370

Tags:**Notes:**

Nothing to report

RHEL-07-030380 (V-72099)

The Red Hat Enterprise Linux operating system must audit all uses of the fchown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030380

Tags:**Notes:**

Nothing to report

RHEL-07-030390 (V-72101)

The Red Hat Enterprise Linux operating system must audit all uses of the lchown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030390

Tags:

--

Notes:

Nothing to report

RHEL-07-030400 (V-72103)

The Red Hat Enterprise Linux operating system must audit all uses of the fchowmat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030400

Tags:

--

Notes:

Nothing to report

RHEL-07-030410 (V-72105)

The Red Hat Enterprise Linux operating system must audit all uses of the chmod syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030410

Tags:

--

Notes:

Nothing to report

RHEL-07-030420 (V-72107)

The Red Hat Enterprise Linux operating system must audit all uses of the fchmod syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030420

Tags:

--

Notes:

Nothing to report

RHEL-07-030430 (V-72109)

The Red Hat Enterprise Linux operating system must audit all uses of the fchmodat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030430

Tags:

--

Notes:

Nothing to report

RHEL-07-030440 (V-72111)

The Red Hat Enterprise Linux operating system must audit all uses of the setxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030440

Tags:

--

Notes:

Nothing to report

RHEL-07-030450 (V-72113)

The Red Hat Enterprise Linux operating system must audit all uses of the fsetxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030450

Tags:

--

Notes:

Nothing to report

RHEL-07-030460 (V-72115)

The Red Hat Enterprise Linux operating system must audit all uses of the lsetxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030460

Tags:

--

Notes:

Nothing to report

RHEL-07-030470 (V-72117)

The Red Hat Enterprise Linux operating system must audit all uses of the removexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030470

Tags:

--

Notes:

Nothing to report

RHEL-07-030480 (V-72119)

The Red Hat Enterprise Linux operating system must audit all uses of the fremovexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030480

Tags:

--

Notes:

Nothing to report

RHEL-07-030490 (V-72121)

The Red Hat Enterprise Linux operating system must audit all uses of the lremovexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

```
rhel_07_030490
```

Tags:

Notes:

Nothing to report

RHEL-07-030500 (V-72123)

The Red Hat Enterprise Linux operating system must audit all uses of the creat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030500  
rhel_07_030500
```

Tags:

Notes:

Nothing to report

RHEL-07-030510 (V-72125)

The Red Hat Enterprise Linux operating system must audit all uses of the open syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030510 rhel_07_030510

Tags:

--

Notes:

Nothing to report

RHEL-07-030520 (V-72127)

The Red Hat Enterprise Linux operating system must audit all uses of the openat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030520 rhel_07_030520

Tags:

--

Notes:

Nothing to report

RHEL-07-030530 (V-72129)

The Red Hat Enterprise Linux operating system must audit all uses of the `open_by_handle_at` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030530
rhel_07_030530
```

Tags:

Notes:

Nothing to report

RHEL-07-030540 (V-72131)

The Red Hat Enterprise Linux operating system must audit all uses of the `truncate` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030540
rhel_07_030540
```

Tags:

Notes:

Nothing to report

RHEL-07-030550 (V-72133)

The Red Hat Enterprise Linux operating system must audit all uses of the ftruncate syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030550
rhel_07_030550
```

Tags:**Notes:**

Nothing to report

RHEL-07-030560 (V-72135)

The Red Hat Enterprise Linux operating system must audit all uses of the semanage command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

```
rhel_07_030560
```

Tags:

Notes:

Nothing to report

RHEL-07-030570 (V-72137)

The Red Hat Enterprise Linux operating system must audit all uses of the setsebool command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030570

Tags:

Notes:

Nothing to report

RHEL-07-030580 (V-72139)

The Red Hat Enterprise Linux operating system must audit all uses of the chcon command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030580

Tags:

Notes:

Nothing to report

RHEL-07-030590 (V-72141)

The Red Hat Enterprise Linux operating system must audit all uses of the setfiles command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030590

Tags:**Notes:**

Nothing to report

RHEL-07-030610 (V-72145)

The Red Hat Enterprise Linux operating system must generate audit records for all unsuccessful account access events.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Variables:

rhel_07_030610

Tags:

Notes:

Nothing to report

RHEL-07-030620 (V-72147)

The Red Hat Enterprise Linux operating system must generate audit records for all successful account access events.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Variables:

rhel_07_030620

Tags:

Notes:

Nothing to report

RHEL-07-030630 (V-72149)

The Red Hat Enterprise Linux operating system must audit all uses of the passwd command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030630

Tags:**Notes:**

Nothing to report

RHEL-07-030640 (V-72151)

The Red Hat Enterprise Linux operating system must audit all uses of the `unix_chkpwd` command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030640

Tags:**Notes:**

Nothing to report

RHEL-07-030650 (V-72153)

The Red Hat Enterprise Linux operating system must audit all uses of the `gpasswd` command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030650

Tags:

Notes:

Nothing to report

RHEL-07-030660 (V-72155)

The Red Hat Enterprise Linux operating system must audit all uses of the chage command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030660

Tags:

Notes:

Nothing to report

RHEL-07-030670 (V-72157)

The Red Hat Enterprise Linux operating system must audit all uses of the userhelper command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030670

Tags:**Notes:**

Nothing to report

RHEL-07-030680 (V-72159)

The Red Hat Enterprise Linux operating system must audit all uses of the su command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030680

Tags:**Notes:**

Nothing to report

RHEL-07-030690 (V-72161)

The Red Hat Enterprise Linux operating system must audit all uses of the sudo command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

```
rhel_07_030690
```

Tags:

Notes:

Nothing to report

RHEL-07-030700 (V-72163)

The Red Hat Enterprise Linux operating system must audit all uses of the sudoers file and all files in the /etc/sudoers.d/ directory.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

```
rhel_07_030700  
rhel_07_030700
```

Tags:

Notes:

Nothing to report

RHEL-07-030710 (V-72165)

The Red Hat Enterprise Linux operating system must audit all uses of the newgrp command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030710

Tags:**Notes:**

Nothing to report

RHEL-07-030720 (V-72167)

The Red Hat Enterprise Linux operating system must audit all uses of the chsh command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030720

Tags:

Notes:

Nothing to report

RHEL-07-030740 (V-72171)

The Red Hat Enterprise Linux operating system must audit all uses of the mount command and syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030740

Tags:**Notes:**

Nothing to report

RHEL-07-030750 (V-72173)

The Red Hat Enterprise Linux operating system must audit all uses of the umount command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030750

Tags:

Notes:

Nothing to report

RHEL-07-030760 (V-72175)

The Red Hat Enterprise Linux operating system must audit all uses of the postdrop command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030760

Tags:**Notes:**

Nothing to report

RHEL-07-030770 (V-72177)

The Red Hat Enterprise Linux operating system must audit all uses of the postqueue command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030770

Tags:**Notes:**

Nothing to report

RHEL-07-030780 (V-72179)

The Red Hat Enterprise Linux operating system must audit all uses of the ssh-keysign command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030780

Tags:**Notes:**

Nothing to report

RHEL-07-030800 (V-72183)

The Red Hat Enterprise Linux operating system must audit all uses of the crontab command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030800

Tags:**Notes:**

Nothing to report

RHEL-07-030810 (V-72185)

The Red Hat Enterprise Linux operating system must audit all uses of the pam_timestamp_check command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Variables:

rhel_07_030810

Tags:**Notes:**

Nothing to report

RHEL-07-030819 (V-78999)

The Red Hat Enterprise Linux operating system must audit all uses of the create_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030819

Tags:

Notes:

Nothing to report

RHEL-07-030820 (V-72187)

The Red Hat Enterprise Linux operating system must audit all uses of the `init_module` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030820

Tags:

Notes:

Nothing to report

RHEL-07-030821 (V-79001)

The Red Hat Enterprise Linux operating system must audit all uses of the `finit_module` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030821

Tags:**Notes:**

Nothing to report

RHEL-07-030830 (V-72189)

The Red Hat Enterprise Linux operating system must audit all uses of the delete_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030830

Tags:**Notes:**

Nothing to report

RHEL-07-030840 (V-72191)

The Red Hat Enterprise Linux operating system must audit all uses of the kmod command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030840

Tags:

Notes:

Nothing to report

RHEL-07-030870 (V-72197)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Variables:

rhel_07_030870

Tags:

Notes:

Nothing to report

RHEL-07-030871 (V-73165)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030871

Tags:**Notes:**

Nothing to report

RHEL-07-030872 (V-73167)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030872

Tags:**Notes:**

Nothing to report

RHEL-07-030873 (V-73171)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030873

Tags:**Notes:**

Nothing to report

RHEL-07-030874 (V-73173)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030874

Tags:**Notes:**

Nothing to report

RHEL-07-030880 (V-72199)

The Red Hat Enterprise Linux operating system must audit all uses of the rename syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030880

Tags:

Notes:

Nothing to report

RHEL-07-030890 (V-72201)

The Red Hat Enterprise Linux operating system must audit all uses of the renameat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030890

Tags:**Notes:**

Nothing to report

RHEL-07-030900 (V-72203)

The Red Hat Enterprise Linux operating system must audit all uses of the rmdir syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030900

Tags:**Notes:**

Nothing to report

RHEL-07-030910 (V-72205)

The Red Hat Enterprise Linux operating system must audit all uses of the unlink syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030910

Tags:

Notes:

Nothing to report

RHEL-07-030920 (V-72207)

The Red Hat Enterprise Linux operating system must audit all uses of the unlinkat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030920

Tags:

Notes:

Nothing to report

RHEL-07-031000 (V-72209)

The Red Hat Enterprise Linux operating system must send rsyslog output to a log aggregation server.

Severity: Medium

Implementation Status: Implemented

Description:

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Variables:

```
rhel_07_031000
rhel7stig_log_aggregation_server is defined
```

Tags:

```
RHEL-07-031000
rsyslog
```

Notes:

Nothing to report

RHEL-07-031010 (V-72211)

The Red Hat Enterprise Linux operating system must be configured so that the rsyslog daemon does not accept log messages from other servers unless the server is being used for log aggregation.

Severity: Medium

Implementation Status: Implemented

Description:

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the system's logs, or could fill the system's storage leading to a Denial of Service.

If the system is intended to be a log aggregation server its use must be documented with the ISSO.

Variables:

```
rhel_07_031010
not rhel7stig_system_is_log_aggregator
```

Tags:

```
RHEL-07-031010
rsyslog
```

Notes:

Nothing to report

RHEL-07-032000 (V-72213)

The Red Hat Enterprise Linux operating system must use a virus scan program.

Severity: High

Implementation Status: Implemented

Description:

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Variables:

```
rhel7stig_antivirus_required  
rhel_07_032000
```

Tags:

```
RHEL-07-032000  
antivirus
```

Notes:

Nothing to report

RHEL-07-040000 (V-72217)

The Red Hat Enterprise Linux operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

Severity: Low

Implementation Status: Implemented

Description:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Variables:

```
rhel_07_040000
```

Tags:

```
RHEL-07-040000
```

Notes:

Nothing to report

RHEL-07-040100 (V-72219)

The Red Hat Enterprise Linux operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.

Severity: Medium

Implementation Status: Not Implemented

Description:

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Variables:

```
rhel_07_040100
```

Tags:

```
RHEL-07-040100  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040110 (V-72221)

The Red Hat Enterprise Linux operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

Severity: Medium

Implementation Status: Implemented

Description:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Variables:

```
rhel_07_040110
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040110
ssh
```

Notes:

Nothing to report

RHEL-07-040160 (V-72223)

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 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Variables:

```
rhel_07_040160
```

Tags:

```
RHEL-07-040160
profile
```

Notes:

Nothing to report

RHEL-07-040170 (V-72225)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner immediately prior to, or as part of, remote access logon prompts.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

```
rhel_07_040170  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040170  
ssh  
dod_logon_banner
```

Notes:

Nothing to report

RHEL-07-040180 (V-72227)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

```
rhel_07_040180
```

Tags:

```
RHEL-07-040180  
ldap  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040190 (V-72229)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_040190

Tags:

RHEL-07-040190 notimplemented

Notes:

Nothing to report

RHEL-07-040200 (V-72231)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_040200

Tags:

RHEL-07-040200 notimplemented

Notes:

Nothing to report

RHEL-07-040201 (V-77825)

The Red Hat Enterprise Linux operating system must implement virtual address space randomization.

Severity: Medium

Implementation Status: Implemented

Description:

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code he or she has introduced into a process's address space during an attempt at exploitation. Additionally, ASLR also makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return-oriented programming (ROP) techniques.

Variables:

```
rhel_07_040201
```

Tags:

```
RHEL-07-040201  
sysctl
```

Notes:

Nothing to report

RHEL-07-040300 (V-72233)

The Red Hat Enterprise Linux operating system must be configured so that all networked systems have SSH installed.

Severity: Medium

Implementation Status: Implemented

Description:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Variables:

```
rhel_07_040300  
rhel7stig_ssh_required
```

Tags:


```
RHEL-07-040300
ssh
```

Notes:

Nothing to report

RHEL-07-040310 (V-72235)

The Red Hat Enterprise Linux operating system must be configured so that all networked systems use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.

Severity: Medium

Implementation Status: Implemented

Description:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000423-GPOS-00188, SRG-OS-000423-GPOS-00189, SRG-OS-000423-GPOS-00190

Variables:

```
rhel_07_040310
rhel7stig_ssh_required
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
```

Tags:

```
RHEL-07-040310
ssh
```

Notes:

Nothing to report

RHEL-07-040320 (V-72237)

The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic are terminated at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Variables:

```
rhel_07_040320
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040320
ssh
```

Notes:

Nothing to report

RHEL-07-040330 (V-72239)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote login via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040330
rhel7stig_ssh_required
ansible_distribution_version is not version_compare('7.4', '>=')
```

Tags:

```
RHEL-07-040330
ssh
```

Notes:

Nothing to report

RHEL-07-040340 (V-72241)

The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic terminate after a period of inactivity.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Variables:

```
rhel_07_040340
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040340
ssh
```

Notes:

Nothing to report

RHEL-07-040350 (V-72243)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using rhosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote login via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040350
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040350
ssh
```

Notes:

Nothing to report

RHEL-07-040360 (V-72245)

The Red Hat Enterprise Linux operating system must display the date and time of the last successful account login upon an SSH login.

Severity: Medium

Implementation Status: Implemented

Description:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Variables:

```
rhel_07_040360
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040360
ssh
```

Notes:

Nothing to report

RHEL-07-040370 (V-72247)

The Red Hat Enterprise Linux operating system must not permit direct logons to the root account using remote access via SSH.

Severity: Medium

Implementation Status: Implemented

Description:

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Variables:

```
rhel_07_040370
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040370
ssh
```

Notes:

Nothing to report

RHEL-07-040380 (V-72249)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040380
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040380
ssh
```

Notes:

Nothing to report

RHEL-07-040390 (V-72251)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon is configured to only use the SSHv2 protocol.

Severity: High

Implementation Status: Implemented

Description:

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_040390
rhel7stig_ssh_required
ansible_distribution_version is not version_compare('7.4', '>=')
```

Tags:

```
RHEL-07-040390
ssh
```

Notes:

Nothing to report

RHEL-07-040400 (V-72253)

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.

Severity: Medium

Implementation Status: Implemented

Description:

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Variables:

```
rhel_07_040400
rhel7stig_ssh_required
```

Tags:

```
ssh
RHEL-07-040400
```

Notes:

Nothing to report

RHEL-07-040410 (V-72255)

The Red Hat Enterprise Linux operating system must be configured so that the SSH public host key files have mode 0644 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Variables:

```
rhel_07_040410
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040410
ssh
```

Notes:

Nothing to report

RHEL-07-040420 (V-72257)

The Red Hat Enterprise Linux operating system must be configured so that the SSH private host key files have mode 0640 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Variables:

```
rhel_07_040420
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040420
ssh
```

Notes:

Nothing to report

RHEL-07-040430 (V-72259)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Variables:

```
rhel_07_040430
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040430
ssh
```

Notes:

Nothing to report

RHEL-07-040440 (V-72261)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Variables:

```
rhel_07_040440
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040440
ssh
```

Notes:

Nothing to report

RHEL-07-040450 (V-72263)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon performs strict mode checking of home directory configuration files.

Severity: Medium

Implementation Status: Implemented

Description:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Variables:

```
rhel_07_040450
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040450
ssh
```

Notes:

Nothing to report

RHEL-07-040460 (V-72265)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon uses privilege separation.

Severity: Medium

Implementation Status: Implemented

Description:

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Variables:

```
rhel_07_040460
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040460
ssh
```

Notes:

Nothing to report

RHEL-07-040470 (V-72267)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.

Severity: Medium

Implementation Status: Implemented

Description:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Variables:

```
rhel_07_040470
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040470
ssh
```

Notes:

Nothing to report

RHEL-07-040500 (V-72269)

The Red Hat Enterprise Linux operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Severity: Medium

Implementation Status: Implemented

Description:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Variables:

```
rhel7stig_time_service == 'ntpd'
rhel_07_040500
rhel7stig_time_service == 'chronyd'
rhel_07_040500
rhel7stig_time_service == 'chronyd'
rhel_07_040500
```

Tags:

```
RHEL-07-040500
chronyd
```

Notes:

Nothing to report

RHEL-07-040510 (V-72271)

The Red Hat Enterprise Linux operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.

Severity: Medium

Implementation Status: Not Implemented

Description:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Variables:**Tags:****Notes:**

Nothing to report

RHEL-07-040520 (V-72273)

The Red Hat Enterprise Linux operating system must enable an application firewall, if available.

Severity: Medium

Implementation Status: Implemented

Description:

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Variables:

```
rhel_07_040520
rhel_07_040520
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
```

Tags:

```
RHEL-07-040520
firewall
```

Notes:

Nothing to report

RHEL-07-040530 (V-72275)

The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon logon.

Severity: Low

Implementation Status: Implemented

Description:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Variables:

```
rhel_07_040530
```

Tags:

```
RHEL-07-040530  
pamd
```

Notes:

Nothing to report

RHEL-07-040540 (V-72277)

The Red Hat Enterprise Linux operating system must not contain .shosts files.

Severity: High

Implementation Status: Implemented

Description:

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Variables:

```
rhel_07_040540
```

Tags:

```
RHEL-07-040540  
shosts
```

Notes:

Nothing to report

RHEL-07-040550 (V-72279)

The Red Hat Enterprise Linux operating system must not contain shosts.equiv files.

Severity: High

Implementation Status: Implemented

Description:

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Variables:

```
rhel_07_040550
```

Tags:

```
RHEL-07-040550  
shosts
```

Notes:

Nothing to report

RHEL-07-040600 (V-72281)

For Red Hat Enterprise Linux operating systems using DNS resolution, at least two name servers must be configured.

Severity: Low

Implementation Status: Not Implemented

Description:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Variables:

```
rhel_07_040600
```

Tags:

```
RHEL-07-040600  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040610 (V-72283)

The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040610
```

Tags:

```
RHEL-07-040610  
ipv4
```

Notes:

Nothing to report

RHEL-07-040620 (V-72285)

The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040620
```

Tags:

`RHEL-07-040620`
`ipv4`

Notes:

Nothing to report

RHEL-07-040630 (V-72287)

The Red Hat Enterprise Linux operating system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

Severity: Medium

Implementation Status: Implemented

Description:

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Variables:

`rhel_07_040630`

Tags:

`RHEL-07-040630`
`ipv4`

Notes:

Nothing to report

RHEL-07-040640 (V-72289)

The Red Hat Enterprise Linux operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Variables:

`rhel_07_040640`

Tags:

```
RHEL-07-040640  
ipv4
```

Notes:

Nothing to report

RHEL-07-040641 (V-73175)

The Red Hat Enterprise Linux operating system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Variables:

```
rhel_07_040641
```

Tags:

```
RHEL-07-040641  
ipv4
```

Notes:

Nothing to report

RHEL-07-040650 (V-72291)

The Red Hat Enterprise Linux operating system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Variables:

```
rhel_07_040650
```

Tags:


```
RHEL-07-040650  
ipv4
```

Notes:

Nothing to report

RHEL-07-040660 (V-72293)

The Red Hat Enterprise Linux operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Variables:

```
rhel_07_040660
```

Tags:

```
RHEL-07-040660  
ipv4
```

Notes:

Nothing to report

RHEL-07-040670 (V-72295)

Network interfaces configured on the Red Hat Enterprise Linux operating system must not be in promiscuous mode.

Severity: Medium

Implementation Status: Implemented

Description:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Variables:

```
rhel_07_040670  
not rhel7stig_net_promisc_mode_required
```

Tags:

RHEL-07-040670

Notes:

Nothing to report

RHEL-07-040680 (V-72297)

The Red Hat Enterprise Linux operating system must be configured to prevent unrestricted mail relaying.

Severity: Medium

Implementation Status: Implemented

Description:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Variables:

rhel_07_040680

Tags:

RHEL-07-040680

Notes:

Nothing to report

RHEL-07-040690 (V-72299)

The Red Hat Enterprise Linux operating system must not have a File Transfer Protocol (FTP) server package installed unless needed.

Severity: High

Implementation Status: Disruption High

Description:

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Variables:

not rhel7stig_vsftpd_required
rhel_07_040690
rhel7stig_disruptive

Tags:

```
RHEL-07-040690  
disruption-high  
ftp
```

Notes:

Nothing to report

RHEL-07-040700 (V-72301)

The Red Hat Enterprise Linux operating system must not have the Trivial File Transfer Protocol (TFTP) server package installed if not required for operational support.

Severity: High

Implementation Status: Disruption High

Description:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Variables:

```
not_rhel7stig_tftp_required  
rhel_07_040700  
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040700  
disruption-high  
tftp
```

Notes:

Nothing to report

RHEL-07-040710 (V-72303)

The Red Hat Enterprise Linux operating system must be configured so that remote X connections for interactive users are encrypted.

Severity: High

Implementation Status: Implemented

Description:

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Variables:

```
rhel_07_040710
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040710
ssh
```

Notes:

Nothing to report

RHEL-07-040720 (V-72305)

The Red Hat Enterprise Linux operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is configured to operate in secure mode.

Severity: Medium

Implementation Status: Implemented

Description:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Variables:

```
rhel7stig_tftp_required
rhel_07_040720
```

Tags:

```
RHEL-07-040720
```

Notes:

Nothing to report

RHEL-07-040730 (V-72307)

The Red Hat Enterprise Linux operating system must not have an X Windows display manager installed unless approved.

Severity: Medium

Implementation Status: Disruption High

Description:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Variables:

```
not rhel7stig_gui
rhel_07_040730
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040730
disruption-high
x11
gui
```

Notes:

Nothing to report

RHEL-07-040740 (V-72309)

The Red Hat Enterprise Linux operating system must not be performing packet forwarding unless the system is a router.

Severity: Medium

Implementation Status: Implemented

Description:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Variables:

```
not rhel7stig_system_is_router
rhel_07_040740
```

Tags:

```
RHEL-07-040740
ipv4
```

Notes:

Nothing to report

RHEL-07-040750 (V-72311)

The Red Hat Enterprise Linux operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.

Severity: Medium

Implementation Status: Not Implemented

Description:

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Variables:

rhel_07_040750

Tags:

RHEL-07-040750 notimplemented

Notes:

Nothing to report

RHEL-07-040800 (V-72313)

SNMP community strings on the Red Hat Enterprise Linux operating system must be changed from the default.

Severity: High

Implementation Status: Implemented

Description:

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Variables:

rhel_07_040800

Tags:

RHEL-07-040800 snmp

Notes:

Nothing to report

RHEL-07-040810 (V-72315)

The Red Hat Enterprise Linux operating system access control program must be configured to grant or deny system access to specific hosts and services.

Severity: Medium

Implementation Status: Not Implemented

Description:

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Variables:

rhel_07_040810

Tags:

RHEL-07-040810 notimplemented

Notes:

Nothing to report

RHEL-07-040820 (V-72317)

The Red Hat Enterprise Linux operating system must not have unauthorized IP tunnels configured.

Severity: Medium

Implementation Status: Disruption High

Description:

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the Information System Security Officer (ISSO).

Variables:

rhel_07_040820 rhel7stig_disruptive
--

Tags:

RHEL-07-040820 disruption-high

Notes:

Nothing to report

RHEL-07-040830 (V-72319)

The Red Hat Enterprise Linux operating system must not forward IPv6 source-routed packets.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040830
```

Tags:

```
RHEL-07-040830  
ipv6
```

Notes:

Nothing to report

RHEL-07-041001 (V-72417)

The Red Hat Enterprise Linux operating system must have the required packages for multifactor authentication installed.

Severity: Medium

Implementation Status: Implemented

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel_07_041001
```

Tags:

```
RHEL-07-041001  
multifactor
```


Notes:

Nothing to report

RHEL-07-041002 (V-72427)

The Red Hat Enterprise Linux operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

Severity: Medium

Implementation Status: Complexity High

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel7stig_auth_settings.use_sssd
rhel7stig_complex
rhel_07_041002
```

Tags:

```
RHEL-07-041002
complexity-high
sssd
```

Notes:

Nothing to report

RHEL-07-041003 (V-72433)

The Red Hat Enterprise Linux operating system must implement certificate status checking for PKI authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel_07_041003
ansible_distribution_major_version is version_compare('8', '<')
```

Tags:

```
RHEL-07-041003
```

Notes:

Nothing to report

RHEL-07-041010 (V-73177)

The Red Hat Enterprise Linux operating system must be configured so that all wireless network adapters are disabled.

Severity: Medium

Implementation Status: Implemented

Description:

The use of wireless networking can introduce many different attack vectors into the organization's network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial of service to valid network resources.

Variables:

```
rhel_07_041010
```

Tags:

```
RHEL-07-041010
```

Notes:

Nothing to report

Controls by Severity**Contents**

- *Controls by Severity*
 - *High (30 controls)*
 - *Medium (199 controls)*
 - *Low (14 controls)*

High (30 controls)**RHEL-07-010010 (V-71849)**

The Red Hat Enterprise Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.

Severity: High

Implementation Status: Implemented

Description:

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Variables:

```
rhel_07_010010
```

Tags:

```
RHEL-07-010010
```

Notes:

Nothing to report

RHEL-07-010020 (V-71855)

The Red Hat Enterprise Linux operating system must be configured so that the cryptographic hash of system files and commands matches vendor values.

Severity: High

Implementation Status: Implemented

Description:

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_010020

Tags:

RHEL-07-010020

Notes:

Nothing to report

RHEL-07-010290 (V-71937)

The Red Hat Enterprise Linux operating system must not have accounts configured with blank or null passwords.

Severity: High

Implementation Status: Implemented

Description:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Variables:

rhel_07_010290

Tags:

RHEL-07-010290
pamd

Notes:

Nothing to report

RHEL-07-010300 (V-71939)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using an empty password.

Severity: High

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_010300
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010300
ssh
```

Notes:

Nothing to report

RHEL-07-010440 (V-71953)

The Red Hat Enterprise Linux operating system must not allow an unattended or automatic logon to the system via a graphical user interface.

Severity: High

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel7stig_gui
rhel_07_010440
```

Tags:

```
RHEL-07-010440
gui
```

Notes:

Nothing to report

RHEL-07-010450 (V-71955)

The Red Hat Enterprise Linux operating system must not allow an unrestricted logon to the system.

Severity: High

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel7stig_gui  
rhel_07_010450
```

Tags:

```
RHEL-07-010450  
gui
```

Notes:

Nothing to report

RHEL-07-010480 (V-71961)

Red Hat Enterprise Linux operating systems prior to version 7.2 with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010480 or rhel_07_010490  
ansible_distribution_version is version_compare('7.2', '<')
```

Tags:

```
RHEL-07-010480  
RHEL-07-010490  
grub  
bootloader
```

Notes:

Nothing to report

RHEL-07-010482 (V-81005)

Red Hat Enterprise Linux operating systems version 7.2 or newer with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010482 or rhel_07_010491
ansible_distribution_version is version_compare('7.2', '>=')
```

Tags:

```
RHEL-07-010482
RHEL-07-010491
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010490 (V-71963)

Red Hat Enterprise Linux operating systems prior to version 7.2 using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010480 or rhel_07_010490
ansible_distribution_version is version_compare('7.2', '<')
```

Tags:

```
RHEL-07-010480
RHEL-07-010490
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010491 (V-81007)

Red Hat Enterprise Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010482 or rhel_07_010491
ansible_distribution_version is version_compare('7.2', '>=')
```

Tags:

```
RHEL-07-010482
RHEL-07-010491
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-020000 (V-71967)

The Red Hat Enterprise Linux operating system must not have the rsh-server package installed.

Severity: High

Implementation Status: Implemented

Description:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Variables:

rhel_07_020000

Tags:

RHEL-07-020000 rsh

Notes:

Nothing to report

RHEL-07-020010 (V-71969)

The Red Hat Enterprise Linux operating system must not have the ypserv package installed.

Severity: High

Implementation Status: Implemented

Description:

Removing the “ypserv” package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Variables:

rhel_07_020010

Tags:

RHEL-07-020010 ypserv

Notes:

Nothing to report

RHEL-07-020050 (V-71977)

The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Severity: High

Implementation Status: Implemented

Description:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Variables:

rhel_07_020050

Tags:

RHEL-07-020050 yum

Notes:

Nothing to report

RHEL-07-020060 (V-71979)

The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Severity: High

Implementation Status: Implemented

Description:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Variables:

rhel_07_020060

Tags:

```
RHEL-07-020060
yum
```

Notes:

Nothing to report

RHEL-07-020210 (V-71989)

The Red Hat Enterprise Linux operating system must enable SELinux.

Severity: High

Implementation Status: Implemented

Description:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Variables:

```
rhel_07_020210 or rhel_07_020220
not rhel7stig_system_is_container
```

Tags:

```
RHEL-07-020210
RHEL-07-020220
selinux
```

Notes:

Nothing to report

RHEL-07-020220 (V-71991)

The Red Hat Enterprise Linux operating system must enable the SELinux targeted policy.

Severity: High

Implementation Status: Implemented

Description:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Variables:

```
rhel_07_020210 or rhel_07_020220
not rhel7stig_system_is_container
```

Tags:

```
RHEL-07-020210
RHEL-07-020220
selinux
```

Notes:

Nothing to report

RHEL-07-020230 (V-71993)

The Red Hat Enterprise Linux operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled.

Severity: High

Implementation Status: Implemented

Description:

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Variables:

```
rhel_07_020230
```

Tags:

```
RHEL-07-020230
```

Notes:

Nothing to report

RHEL-07-020250 (V-71997)

The Red Hat Enterprise Linux operating system must be a vendor supported release.

Severity: High

Implementation Status: Complexity High

Description:

An operating system release is considered “supported” if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Variables:

```
rhel_07_020250
rhel7stig_complex
```

Tags:

```
RHEL-07-020250
complexity-high
```

Notes:

Nothing to report

RHEL-07-020310 (V-72005)

The Red Hat Enterprise Linux operating system must be configured so that the root account must be the only account having unrestricted access to the system.

Severity: High

Implementation Status: Implemented

Description:

If an account other than root also has a User Identifier (UID) of “0”, it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of “0” afford an opportunity for potential intruders to guess a password for a privileged account.

Variables:

```
rhel_07_020310
```

Tags:

```
RHEL-07-020310
```

Notes:

Nothing to report

RHEL-07-021350 (V-72067)

The Red Hat Enterprise Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Severity: High

Implementation Status: Implemented

Description:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Variables:

```
rhel_07_021350
ansible_distribution_major_version == '7'
```

Tags:

```
RHEL-07-021350
```

Notes:

Nothing to report

RHEL-07-021710 (V-72077)

The Red Hat Enterprise Linux operating system must not have the telnet-server package installed.

Severity: High

Implementation Status: Implemented

Description:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Variables:

```
rhel_07_021710
```

Tags:

```
RHEL-07-021710
telnet
```

Notes:

Nothing to report

RHEL-07-030000 (V-72079)

The Red Hat Enterprise Linux operating system must be configured so that auditing is configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.

Severity: High

Implementation Status: Implemented

Description:

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096

Variables:

`rhel_07_030000`

Tags:

`RHEL-07-030000`
`auditd`

Notes:

Nothing to report

RHEL-07-032000 (V-72213)

The Red Hat Enterprise Linux operating system must use a virus scan program.

Severity: High

Implementation Status: Implemented

Description:

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Variables:

```
rhel7stig_antivirus_required  
rhel_07_032000
```

Tags:

```
RHEL-07-032000  
antivirus
```

Notes:

Nothing to report

RHEL-07-040390 (V-72251)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon is configured to only use the SSHv2 protocol.

Severity: High

Implementation Status: Implemented

Description:

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_040390  
rhel7stig_ssh_required  
ansible_distribution_version is not version_compare('7.4', '>=')
```

Tags:

```
RHEL-07-040390  
ssh
```

Notes:

Nothing to report

RHEL-07-040540 (V-72277)

The Red Hat Enterprise Linux operating system must not contain .shosts files.

Severity: High

Implementation Status: Implemented

Description:

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Variables:

rhel_07_040540

Tags:

RHEL-07-040540 shosts

Notes:

Nothing to report

RHEL-07-040550 (V-72279)

The Red Hat Enterprise Linux operating system must not contain shosts.equiv files.

Severity: High

Implementation Status: Implemented

Description:

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Variables:

rhel_07_040550

Tags:

RHEL-07-040550 shosts

Notes:

Nothing to report

RHEL-07-040690 (V-72299)

The Red Hat Enterprise Linux operating system must not have a File Transfer Protocol (FTP) server package installed unless needed.

Severity: High

Implementation Status: Disruption High

Description:

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Variables:

```
not rhel7stig_vsftpd_required
rhel_07_040690
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040690
disruption-high
ftp
```

Notes:

Nothing to report

RHEL-07-040700 (V-72301)

The Red Hat Enterprise Linux operating system must not have the Trivial File Transfer Protocol (TFTP) server package installed if not required for operational support.

Severity: High

Implementation Status: Disruption High

Description:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Variables:

```
not rhel7stig_tftp_required
rhel_07_040700
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040700
disruption-high
tftp
```

Notes:

Nothing to report

RHEL-07-040710 (V-72303)

The Red Hat Enterprise Linux operating system must be configured so that remote X connections for interactive users are encrypted.

Severity: High

Implementation Status: Implemented

Description:

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Variables:

```
rhel_07_040710
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040710
ssh
```

Notes:

Nothing to report

RHEL-07-040800 (V-72313)

SNMP community strings on the Red Hat Enterprise Linux operating system must be changed from the default.

Severity: High

Implementation Status: Implemented

Description:

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Variables:

```
rhel_07_040800
```

Tags:

```
RHEL-07-040800
snmp
```

Notes:

Nothing to report

Medium (199 controls)

RHEL-07-010030 (V-71859)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

```
rhel7stig_dconf_available  
rhel_07_010030  
rhel_07_010040
```

Tags:

```
RHEL-07-010030  
RHEL_07_010040  
dod_logon_banner  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010040 (V-71861)

The Red Hat Enterprise Linux operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

Severity: Medium

Implementation Status: Not Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)  
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),  
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this  
IS for purposes including, but not limited to, penetration  
testing, COMSEC monitoring, network operations and defense,  
personnel misconduct (PM), law enforcement (LE), and  
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this  
IS.
```

```
-Communications using, or data stored on, this IS are not private,  
are subject to routine monitoring, interception, and search, and  
may be disclosed or used for any USG-authorized purpose.
```

(continues on next page)

(continued from previous page)

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

Tags:

Notes:

Nothing to report

RHEL-07-010050 (V-71863)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this

(continues on next page)

(continued from previous page)

IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Variables:

```
rhel_07_010050
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010050
ssh
dod_logon_banner
```

Notes:

Nothing to report

RHEL-07-010060 (V-71891)

The Red Hat Enterprise Linux operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures.

Severity: Medium

Implementation Status: Implemented

Description:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Variables:

```
rhel7stig_dconf_available  
rhel_07_010060
```

Tags:

```
RHEL-07-010060  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010061 (V-77819)

The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.

Severity: Medium

Implementation Status: Implemented

Description:

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Variables:

```
rhel7stig_dconf_available  
rhel_07_010061
```

Tags:

```
RHEL-07-010061  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010070 (V-71893)

The Red Hat Enterprise Linux operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available
rhel_07_010070
```

Tags:

```
RHEL-07-010070
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010081 (V-73155)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver lock-delay setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available
rhel_07_010081
```

Tags:

```
RHEL-07-010081
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010082 (V-73157)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available
rhel_07_010082
```

Tags:

```
RHEL-07-010082
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010090 (V-71897)

The Red Hat Enterprise Linux operating system must have the screen package installed.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The screen package allows for a session lock to be implemented and configured.

Variables:

rhel_07_010090

Tags:

RHEL-07-010090

Notes:

Nothing to report

RHEL-07-010100 (V-71899)

The Red Hat Enterprise Linux operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

rhel7stig_dconf_available
rhel_07_010100

Tags:

RHEL-07-010100
dconf
gui

Notes:

Nothing to report

RHEL-07-010101 (V-78997)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010101
```

Tags:

```
RHEL-07-010101  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010110 (V-71901)

The Red Hat Enterprise Linux operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010110
```

Tags:

```
RHEL-07-010110  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010118 (V-81003)

The Red Hat Enterprise Linux operating system must be configured so that /etc/pam.d/passwd implements /etc/pam.d/system-auth when changing passwords.

Severity: Medium

Implementation Status: Not Implemented

Description:

Pluggable authentication modules (PAM) allow for a modular approach to integrating authentication methods. PAM operates in a top-down processing model and if the modules are not listed in the correct order, an important security function could be bypassed if stack entries are not centralized.

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-010119 (V-73159)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. “pwquality” enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

Variables:

rhel_07_010119

Tags:

RHEL-07-010119 pamd

Notes:

Nothing to report

RHEL-07-010120 (V-71903)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one upper-case character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010120
```

Tags:

```
RHEL-07-010120  
pwquality
```

Notes:

Nothing to report

RHEL-07-010130 (V-71905)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one lower-case character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010130
```

Tags:

RHEL-07-010130 pwquality

Notes:

Nothing to report

RHEL-07-010140 (V-71907)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

rhel_07_010140

Tags:

RHEL-07-010140 pwquality

Notes:

Nothing to report

RHEL-07-010150 (V-71909)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one special character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010150
```

Tags:

```
RHEL-07-010150  
pwquality
```

Notes:

Nothing to report

RHEL-07-010160 (V-71911)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of eight of the total number of characters must be changed.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010160
```

Tags:

```
RHEL-07-010160  
pwquality
```

Notes:

Nothing to report

RHEL-07-010170 (V-71913)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of four character classes must be changed.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010170
```

Tags:

```
RHEL-07-010170  
pwquality
```

Notes:

Nothing to report

RHEL-07-010180 (V-71915)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed the number of repeating consecutive characters must not be more than three characters.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010180
```

Tags:

```
RHEL-07-010180  
pwquality
```

Notes:

Nothing to report

RHEL-07-010190 (V-71917)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010190
```

Tags:

```
RHEL-07-010190  
pwquality
```

Notes:

Nothing to report

RHEL-07-010200 (V-71919)

The Red Hat Enterprise Linux operating system must be configured so that the PAM system service is configured to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

```
rhel_07_010200
```

Tags:

```
RHEL-07-010200  
pamd
```

Notes:

Nothing to report

RHEL-07-010210 (V-71921)

The Red Hat Enterprise Linux operating system must be configured to use the shadow file to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

rhel_07_010210

Tags:

RHEL-07-010210
login

Notes:

Nothing to report

RHEL-07-010220 (V-71923)

The Red Hat Enterprise Linux operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

rhel_07_010220

Tags:

RHEL-07-010220

Notes:

Nothing to report

RHEL-07-010230 (V-71925)

The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 24 hours/1 day minimum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Variables:

rhel_07_010230

Tags:

RHEL-07-010230
login

Notes:

Nothing to report

RHEL-07-010240 (V-71927)

The Red Hat Enterprise Linux operating system must be configured so that passwords are restricted to a 24 hours/1 day minimum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Variables:

rhel_07_010240

Tags:

```
RHEL-07-010240
password
```

Notes:

Nothing to report

RHEL-07-010250 (V-71929)

The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 60-day maximum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Variables:

```
rhel_07_010250
```

Tags:

```
RHEL-07-010250
login
```

Notes:

Nothing to report

RHEL-07-010260 (V-71931)

The Red Hat Enterprise Linux operating system must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

Severity: Medium

Implementation Status: Disruption High

Description:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Variables:

```
rhel_07_010260
rhel7stig_disruptive
```

Tags:

```
RHEL-07-010260  
disruption-high  
password
```

Notes:

Nothing to report

RHEL-07-010270 (V-71933)

The Red Hat Enterprise Linux operating system must be configured so that passwords are prohibited from reuse for a minimum of five generations.

Severity: Medium

Implementation Status: Implemented

Description:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Variables:

```
rhel_07_010270
```

Tags:

```
RHEL-07-010270  
pamd
```

Notes:

Nothing to report

RHEL-07-010280 (V-71935)

The Red Hat Enterprise Linux operating system must be configured so that passwords are a minimum of 15 characters in length.

Severity: Medium

Implementation Status: Implemented

Description:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes

to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Variables:

rhel_07_010280

Tags:

RHEL-07-010280 pwquality

Notes:

Nothing to report

RHEL-07-010310 (V-71941)

The Red Hat Enterprise Linux operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

Severity: Medium

Implementation Status: Implemented

Description:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Variables:

rhel_07_010310

Tags:

RHEL-07-010310

Notes:

Nothing to report

RHEL-07-010320 (V-71943)

Accounts on the Red Hat Enterprise Linux operating system that are subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period.

Severity: Medium

Implementation Status: Implemented

Description:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Variables:

```
rhel_07_010320 or rhel_07_010330
```

Tags:

```
RHEL-07-010320  
RHEL-07-010330  
pamd
```

Notes:

Nothing to report

RHEL-07-010330 (V-71945)

The Red Hat Enterprise Linux operating system must lock the associated account after three unsuccessful root logon attempts are made within a 15-minute period.

Severity: Medium

Implementation Status: Implemented

Description:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Variables:

```
rhel_07_010320 or rhel_07_010330
```

Tags:

```
RHEL-07-010320  
RHEL-07-010330  
pamd
```

Notes:

Nothing to report

RHEL-07-010340 (V-71947)

The Red Hat Enterprise Linux operating system must be configured so that users must provide a password for privilege escalation.

Severity: Medium

Implementation Status: Implemented

Description:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Variables:

```
rhel7stig_using_password_auth
rhel_07_010340
```

Tags:

```
RHEL-07-010340
sudoers
```

Notes:

Nothing to report

RHEL-07-010350 (V-71949)

The Red Hat Enterprise Linux operating system must be configured so that users must re-authenticate for privilege escalation.

Severity: Medium

Implementation Status: Implemented

Description:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Variables:

```
rhel_07_010350
```

Tags:

```
RHEL-07-010350
sudoers
```

Notes:

Nothing to report

RHEL-07-010430 (V-71951)

The Red Hat Enterprise Linux operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Variables:

```
rhel_07_010430
```

Tags:

```
RHEL-07-010430  
login
```

Notes:

Nothing to report

RHEL-07-010460 (V-71957)

The Red Hat Enterprise Linux operating system must not allow users to override SSH environment variables.

Severity: Medium

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel_07_010460  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010460  
ssh
```

Notes:

Nothing to report

RHEL-07-010470 (V-71959)

The Red Hat Enterprise Linux operating system must not allow a non-certificate trusted host SSH logon to the system.

Severity: Medium

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

rhel7stig_ssh_required

Tags:

RHEL-07-010470 ssh

Notes:

Nothing to report

RHEL-07-010481 (V-77823)

The Red Hat Enterprise Linux operating system must require authentication upon booting into single-user and maintenance modes.

Severity: Medium

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Variables:

rhel_07_010481

Tags:

RHEL-07-010481 rescue

Notes:

Nothing to report

RHEL-07-010500 (V-71965)

The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.

Severity: Medium

Implementation Status: Not Implemented

Description:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

- 1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication;

and

- 2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Variables:

```
rhel_07_010500
```

Tags:

```
RHEL-07-010500  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020020 (V-71971)

The Red Hat Enterprise Linux operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Severity: Medium

Implementation Status: Not Implemented

Description:

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Variables:

`rhel_07_020020`

Tags:

`RHEL-07-020020`
`notimplemented`

Notes:

Nothing to report

RHEL-07-020030 (V-71973)

The Red Hat Enterprise Linux operating system must be configured so that a file integrity tool verifies the baseline operating system configuration at least weekly.

Severity: Medium

Implementation Status: Implemented

Description:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Variables:

`rhel_07_020030 or rhel_07_020040`

Tags:

`RHEL-07-020030`
`RHEL-07-020040`
`aide`

Notes:

Nothing to report

RHEL-07-020040 (V-71975)

The Red Hat Enterprise Linux operating system must be configured so that designated personnel are notified if baseline configurations are changed in an unauthorized manner.

Severity: Medium

Implementation Status: Implemented

Description:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Variables:

```
rhel_07_020030 or rhel_07_020040
```

Tags:

```
RHEL-07-020030  
RHEL-07-020040  
aide
```

Notes:

Nothing to report

RHEL-07-020100 (V-71983)

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

Severity: Medium

Implementation Status: Implemented

Description:

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_020100
```

Tags:

```
RHEL-07-020100  
usb_devices
```

Notes:

Nothing to report

RHEL-07-020101 (V-77821)

The Red Hat Enterprise Linux operating system must be configured so that the Datagram Congestion Control Protocol (DCCP) kernel module is disabled unless required.

Severity: Medium

Implementation Status: Implemented

Description:

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Variables:

```
rhel_07_020101
```

Tags:

```
RHEL-07-020101  
dccp
```

Notes:

Nothing to report

RHEL-07-020110 (V-71985)

The Red Hat Enterprise Linux operating system must disable the file system automounter unless required.

Severity: Medium

Implementation Status: Implemented

Description:

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_020110  
rhel_07_020110  
rhel_07_020110_autofs_service_status.stdout == "loaded"  
not rhel7stig_autofs_required
```

Tags:

```
RHEL-07-020110
```

Notes:

Nothing to report

RHEL-07-020240 (V-71995)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Variables:

```
rhel_07_020240
```

Tags:

```
RHEL-07-020240  
login  
umask
```

Notes:

Nothing to report

RHEL-07-020260 (V-71999)

The Red Hat Enterprise Linux operating system security patches and updates must be installed and up to date.

Severity: Medium

Implementation Status: Implemented

Description:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Variables:

```
rhel_07_020260  
rhel_07_020260  
rhel_07_020260  
rhel7stig_auto_package_updates_enabled or rhel_07_020260_yum_cron_installed.rc == 0
```


Tags:

RHEL-07-020260
packaging

Notes:

Nothing to report

RHEL-07-020270 (V-72001)

The Red Hat Enterprise Linux operating system must not have unnecessary accounts.

Severity: Medium

Implementation Status: Implemented

Description:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Variables:

rhel_07_020270

Tags:

RHEL-07-020270

Notes:

Nothing to report

RHEL-07-020320 (V-72007)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid owner.

Severity: Medium

Implementation Status: Complexity High

Description:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier “UID” as the UID of the un-owned files.

Variables:

rhel_07_020320
rhel7stig_complex

Tags:

```
RHEL-07-020320
complexity-high
```

Notes:

Nothing to report

RHEL-07-020330 (V-72009)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid group owner.

Severity: Medium

Implementation Status: Complexity High

Description:

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Variables:

```
rhel_07_020330
rhel7stig_complex
```

Tags:

```
RHEL-07-020330
complexity-high
```

Notes:

Nothing to report

RHEL-07-020600 (V-72011)

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.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Variables:

```
rhel_07_020600
```

Tags:

`RHEL-07-020600`

Notes:

Nothing to report

RHEL-07-020610 (V-72013)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Variables:

`rhel_07_020610`

Tags:

`RHEL-07-020610`
`login`
`home`

Notes:

Nothing to report

RHEL-07-020620 (V-72015)

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.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the `/` directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Variables:

`rhel_07_020620`
`item.uid >= 1000`
`item.uid != 65534`

Tags:

RHEL-07-020620

Notes:

Nothing to report

RHEL-07-020630 (V-72017)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories have mode 0750 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Variables:

rhel_07_020630
item.uid >= 1000
item.uid != 65534

Tags:

RHEL-07-020630

Notes:

Nothing to report

RHEL-07-020640 (V-72019)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are owned by their respective users.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user does not own their home directory, unauthorized users could access or modify the user's files, and the users may not be able to access their own files.

Variables:

rhel_07_020640
item.uid >= 1000
item.uid != 65534

Tags:

RHEL-07-020640

Notes:

Nothing to report

RHEL-07-020650 (V-72021)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners primary group.

Severity: Medium

Implementation Status: Implemented

Description:

If the Group Identifier (GID) of a local interactive user's home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

Variables:

rhel_07_020650
item.uid >= 1000
item.uid != 65534

Tags:

RHEL-07-020650

Notes:

Nothing to report

RHEL-07-020660 (V-72023)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are owned by the owner of the home directory.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Variables:

rhel_07_020660

Tags:

RHEL-07-020660

Notes:

Nothing to report

RHEL-07-020670 (V-72025)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Variables:

rhel_07_020670

Tags:

RHEL-07-020670

Notes:

Nothing to report

RHEL-07-020680 (V-72027)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Variables:

rhel_07_020680

Tags:

RHEL-07-020680

Notes:

Nothing to report

RHEL-07-020690 (V-72029)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for interactive users are owned by the home directory user or root.

Severity: Medium

Implementation Status: Implemented

Description:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020690

Tags:

RHEL-07-020690

Notes:

Nothing to report

RHEL-07-020700 (V-72031)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for local interactive users are be group-owned by the users primary group or root.

Severity: Medium

Implementation Status: Implemented

Description:

Local initialization files for interactive users are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020700

Tags:

RHEL-07-020700

Notes:

Nothing to report

RHEL-07-020710 (V-72033)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files have mode 0740 or less permissive.

Severity: Medium

Implementation Status: Not Implemented

Description:

Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon login.

Variables:

```
rhel_07_020710
```

Tags:

```
RHEL-07-020710  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020720 (V-72035)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user initialization files executable search paths contain only paths that resolve to the users home directory.

Severity: Medium

Implementation Status: Not Implemented

Description:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Variables:

```
rhel_07_020720
```

Tags:

```
RHEL-07-020720  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020730 (V-72037)

The Red Hat Enterprise Linux operating system must be configured so that local initialization files do not execute world-writable programs.

Severity: Medium

Implementation Status: Not Implemented

Description:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Variables:

```
rhel_07_020730
```

Tags:

```
RHEL-07-020730  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020900 (V-72039)

The Red Hat Enterprise Linux operating system must be configured so that all system device files are correctly labeled to prevent unauthorized modification.

Severity: Medium

Implementation Status: Complexity High

Description:

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Variables:

```
rhel_07_020900  
rhel7stig_complex  
ansible_selinux is not defined  
rhel_07_020900  
rhel7stig_complex  
ansible_selinux.status == "enabled"
```

Tags:

```
RHEL-07-020900  
complexity-high
```

Notes:

Nothing to report

RHEL-07-021000 (V-72041)

The Red Hat Enterprise Linux operating system must be configured so that file systems containing user home directories are mounted to prevent files with the setuid and setgid bit set from being executed.

Severity: Medium

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setgid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021000
ansible_mounts | selectattr('mount', 'match', '^/home$') | list | length != 0
'nosuid' not in home_mount.options
```

Tags:

```
RHEL-07-021000
```

Notes:

Nothing to report

RHEL-07-021010 (V-72043)

The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are used with removable media.

Severity: Medium

Implementation Status: Not Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021010
```

Tags:

```
RHEL-07-021010  
notimplemented
```

Notes:

Nothing to report

RHEL-07-021020 (V-72045)

The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are being imported via Network File System (NFS).

Severity: Medium

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021020  
'nosuid' not in (ansible_mounts | json_query(options_query))
```

Tags:

```
RHEL-07-021020
```

Notes:

Nothing to report

RHEL-07-021021 (V-73161)

The Red Hat Enterprise Linux operating system must prevent binary files from being executed on file systems that are being imported via Network File System (NFS).

Severity: Medium

Implementation Status: Implemented

Description:

The “noexec” mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021021  
'noexec' not in (ansible_mounts | json_query(options_query))
```

Tags:

RHEL-07-021021

Notes:

Nothing to report

RHEL-07-021030 (V-72047)

The Red Hat Enterprise Linux operating system must be configured so that all world-writable directories are group-owned by root, sys, bin, or an application group.

Severity: Medium

Implementation Status: Disruption High

Description:

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Variables:

rhel_07_021030
rhel7stig_disruptive

Tags:

RHEL-07-021030
disruption-high

Notes:

Nothing to report

RHEL-07-021040 (V-72049)

The Red Hat Enterprise Linux operating system must set the umask value to 077 for all local interactive user accounts.

Severity: Medium

Implementation Status: Not Implemented

Description:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be “0”. This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Variables:

`rhel_07_021040`

Tags:

`RHEL-07-021040`
`notimplemented`

Notes:

Nothing to report

RHEL-07-021100 (V-72051)

The Red Hat Enterprise Linux operating system must have cron logging implemented.

Severity: Medium

Implementation Status: Implemented

Description:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Variables:

`rhel_07_021100`

Tags:

`RHEL-07-021100`

Notes:

Nothing to report

RHEL-07-021110 (V-72053)

The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is owned by root.

Severity: Medium

Implementation Status: Implemented

Description:

If the owner of the “cron.allow” file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Variables:

`rhel_07_021110`
`rhel_07_021120`

Tags:

```
RHEL-07-021110  
RHEL-07-021120  
cron
```

Notes:

Nothing to report

RHEL-07-021120 (V-72055)

The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is group-owned by root.

Severity: Medium

Implementation Status: Implemented

Description:

If the group owner of the “cron.allow” file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Variables:

```
rhel_07_021110  
rhel_07_021120
```

Tags:

```
RHEL-07-021110  
RHEL-07-021120  
cron
```

Notes:

Nothing to report

RHEL-07-021300 (V-72057)

The Red Hat Enterprise Linux operating system must disable Kernel core dumps unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Variables:

`rhel_07_021300`

Tags:

`RHEL-07-021300`

Notes:

Nothing to report

RHEL-07-021620 (V-72073)

The Red Hat Enterprise Linux operating system must use a file integrity tool that is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Severity: Medium

Implementation Status: Implemented

Description:

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Variables:

`rhel_07_021620`

Tags:

`aide`
`RHEL-07-021620`

Notes:

Nothing to report

RHEL-07-021700 (V-72075)

The Red Hat Enterprise Linux operating system must not allow removable media to be used as the boot loader unless approved.

Severity: Medium

Implementation Status: Not Implemented

Description:

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Variables:

```
rhel_07_021700
```

Tags:

```
RHEL-07-021700  
notimplemented
```

Notes:

Nothing to report

RHEL-07-030010 (V-72081)

The Red Hat Enterprise Linux operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.

Severity: Medium

Implementation Status: Implemented

Description:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Variables:

```
rhel_07_030010
```

Tags:

```
auditd  
RHEL-07-030010
```

Notes:

Nothing to report

RHEL-07-030200 (V-81015)

The Red Hat Enterprise Linux operating system must be configured to use the au-remote plugin.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the “au-remote” plugin, the audisp-remote daemon will not off-load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

rhel_07_030200

Tags:

auditd RHEL-07-030200

Notes:

Nothing to report

RHEL-07-030201 (V-81017)

The Red Hat Enterprise Linux operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the “au-remote” plugin, the audisp-remote daemon will not off load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030210 (V-81019)

The Red Hat Enterprise Linux operating system must take appropriate action when the audisp-remote buffer is full.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When the remote buffer is full, audit logs will not be collected and sent to the central log server.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030211 (V-81021)

The Red Hat Enterprise Linux operating system must label all off-loaded audit logs before sending them to the central log server.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030300 (V-72083)

The Red Hat Enterprise Linux operating system must off-load audit records onto a different system or media from the system being audited.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

```
rhel_07_030300 and rhel7stig_audisp_remote_server
```

Tags:

```
auditd  
RHEL-07-030300
```

Notes:

Nothing to report

RHEL-07-030310 (V-72085)

The Red Hat Enterprise Linux operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

```
rhel_07_030310
```

Tags:

```
auditd  
RHEL-07-030310
```

Notes:

Nothing to report

RHEL-07-030320 (V-72087)

The Red Hat Enterprise Linux operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.

Severity: Medium

Implementation Status: Implemented

Description:

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Variables:

```
rhel_07_030320
```

Tags:

```
auditd  
RHEL-07-030320
```

Notes:

Nothing to report

RHEL-07-030321 (V-73163)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Variables:

```
rhel_07_030321
```

Tags:

```
auditd  
RHEL-07-030321
```

Notes:

Nothing to report

RHEL-07-030330 (V-72089)

The Red Hat Enterprise Linux operating system must initiate an action to notify the System Administrator (SA) and Information System Security Officer ISSO, at a minimum, when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Variables:

```
rhel_07_030330
```

Tags:

```
auditd  
RHEL-07-030330
```

Notes:

Nothing to report

RHEL-07-030340 (V-72091)

The Red Hat Enterprise Linux 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.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Variables:

```
rhel_07_030340
```

Tags:

```
auditd  
RHEL-07-030340
```

Notes:

Nothing to report

RHEL-07-030350 (V-72093)

The Red Hat Enterprise Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Variables:

```
rhel_07_030350
```

Tags:

```
auditd  
RHEL-07-030350
```

Notes:

Nothing to report

RHEL-07-030360 (V-72095)

The Red Hat Enterprise Linux operating system must audit all executions of privileged functions.

Severity: Medium

Implementation Status: Implemented

Description:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Variables:

```
rhel_07_030360
```

Tags:

```
audit-rules  
RHEL-07-030360
```

Notes:

Nothing to report

RHEL-07-030370 (V-72097)

The Red Hat Enterprise Linux operating system must audit all uses of the chown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030370

Tags:**Notes:**

Nothing to report

RHEL-07-030380 (V-72099)

The Red Hat Enterprise Linux operating system must audit all uses of the fchown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030380

Tags:

Notes:

Nothing to report

RHEL-07-030390 (V-72101)

The Red Hat Enterprise Linux operating system must audit all uses of the lchown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030390

Tags:

Notes:

Nothing to report

RHEL-07-030400 (V-72103)

The Red Hat Enterprise Linux operating system must audit all uses of the fchownat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030400

Tags:**Notes:**

Nothing to report

RHEL-07-030410 (V-72105)

The Red Hat Enterprise Linux operating system must audit all uses of the chmod syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030410

Tags:**Notes:**

Nothing to report

RHEL-07-030420 (V-72107)

The Red Hat Enterprise Linux operating system must audit all uses of the fchmod syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030420

Tags:**Notes:**

Nothing to report

RHEL-07-030430 (V-72109)

The Red Hat Enterprise Linux operating system must audit all uses of the fchmodat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030430

Tags:**Notes:**

Nothing to report

RHEL-07-030440 (V-72111)

The Red Hat Enterprise Linux operating system must audit all uses of the setxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030440

Tags:**Notes:**

Nothing to report

RHEL-07-030450 (V-72113)

The Red Hat Enterprise Linux operating system must audit all uses of the fsetxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030450

Tags:**Notes:**

Nothing to report

RHEL-07-030460 (V-72115)

The Red Hat Enterprise Linux operating system must audit all uses of the lsetxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030460

Tags:

Notes:

Nothing to report

RHEL-07-030470 (V-72117)

The Red Hat Enterprise Linux operating system must audit all uses of the removexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030470

Tags:

Notes:

Nothing to report

RHEL-07-030480 (V-72119)

The Red Hat Enterprise Linux operating system must audit all uses of the fremovexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030480

Tags:**Notes:**

Nothing to report

RHEL-07-030490 (V-72121)

The Red Hat Enterprise Linux operating system must audit all uses of the lremovexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030490

Tags:**Notes:**

Nothing to report

RHEL-07-030500 (V-72123)

The Red Hat Enterprise Linux operating system must audit all uses of the creat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030500  
rhel_07_030500
```

Tags:**Notes:**

Nothing to report

RHEL-07-030510 (V-72125)

The Red Hat Enterprise Linux operating system must audit all uses of the open syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030510  
rhel_07_030510
```

Tags:**Notes:**

Nothing to report

RHEL-07-030520 (V-72127)

The Red Hat Enterprise Linux operating system must audit all uses of the openat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030520  
rhel_07_030520
```

Tags:**Notes:**

Nothing to report

RHEL-07-030530 (V-72129)

The Red Hat Enterprise Linux operating system must audit all uses of the open_by_handle_at syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030530  
rhel_07_030530
```

Tags:**Notes:**

Nothing to report

RHEL-07-030540 (V-72131)

The Red Hat Enterprise Linux operating system must audit all uses of the truncate syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030540
rhel_07_030540
```

Tags:

Notes:

Nothing to report

RHEL-07-030550 (V-72133)

The Red Hat Enterprise Linux operating system must audit all uses of the fruncate syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030550
rhel_07_030550
```

Tags:

Notes:

Nothing to report

RHEL-07-030560 (V-72135)

The Red Hat Enterprise Linux operating system must audit all uses of the semanage command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030560

Tags:

--

Notes:

Nothing to report

RHEL-07-030570 (V-72137)

The Red Hat Enterprise Linux operating system must audit all uses of the setsebool command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030570

Tags:

--

Notes:

Nothing to report

RHEL-07-030580 (V-72139)

The Red Hat Enterprise Linux operating system must audit all uses of the chcon command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030580

Tags:

Notes:

Nothing to report

RHEL-07-030590 (V-72141)

The Red Hat Enterprise Linux operating system must audit all uses of the setfiles command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030590

Tags:

Notes:

Nothing to report

RHEL-07-030610 (V-72145)

The Red Hat Enterprise Linux operating system must generate audit records for all unsuccessful account access events.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Variables:

rhel_07_030610

Tags:**Notes:**

Nothing to report

RHEL-07-030620 (V-72147)

The Red Hat Enterprise Linux operating system must generate audit records for all successful account access events.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Variables:

rhel_07_030620

Tags:**Notes:**

Nothing to report

RHEL-07-030630 (V-72149)

The Red Hat Enterprise Linux operating system must audit all uses of the `passwd` command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

<code>rhel_07_030630</code>

Tags:

--

Notes:

Nothing to report

RHEL-07-030640 (V-72151)

The Red Hat Enterprise Linux operating system must audit all uses of the `unix_chkpwd` command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

<code>rhel_07_030640</code>

Tags:

--

Notes:

Nothing to report

RHEL-07-030650 (V-72153)

The Red Hat Enterprise Linux operating system must audit all uses of the gpasswd command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030650

Tags:

Notes:

Nothing to report

RHEL-07-030660 (V-72155)

The Red Hat Enterprise Linux operating system must audit all uses of the chage command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030660

Tags:

Notes:

Nothing to report

RHEL-07-030670 (V-72157)

The Red Hat Enterprise Linux operating system must audit all uses of the userhelper command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030670

Tags:

--

Notes:

Nothing to report

RHEL-07-030680 (V-72159)

The Red Hat Enterprise Linux operating system must audit all uses of the su command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030680

Tags:

--

Notes:

Nothing to report

RHEL-07-030690 (V-72161)

The Red Hat Enterprise Linux operating system must audit all uses of the sudo command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030690

Tags:

--

Notes:

Nothing to report

RHEL-07-030700 (V-72163)

The Red Hat Enterprise Linux operating system must audit all uses of the sudoers file and all files in the /etc/sudoers.d/ directory.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

```
rhel_07_030700  
rhel_07_030700
```

Tags:**Notes:**

Nothing to report

RHEL-07-030710 (V-72165)

The Red Hat Enterprise Linux operating system must audit all uses of the newgrp command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

```
rhel_07_030710
```

Tags:**Notes:**

Nothing to report

RHEL-07-030720 (V-72167)

The Red Hat Enterprise Linux operating system must audit all uses of the chsh command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030720

Tags:

--

Notes:

Nothing to report

RHEL-07-030740 (V-72171)

The Red Hat Enterprise Linux operating system must audit all uses of the mount command and syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030740

Tags:

--

Notes:

Nothing to report

RHEL-07-030750 (V-72173)

The Red Hat Enterprise Linux operating system must audit all uses of the umount command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030750

Tags:

--

Notes:

Nothing to report

RHEL-07-030760 (V-72175)

The Red Hat Enterprise Linux operating system must audit all uses of the postdrop command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030760

Tags:

--

Notes:

Nothing to report

RHEL-07-030770 (V-72177)

The Red Hat Enterprise Linux operating system must audit all uses of the postqueue command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030770

Tags:

--

Notes:

Nothing to report

RHEL-07-030780 (V-72179)

The Red Hat Enterprise Linux operating system must audit all uses of the ssh-keysign command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030780

Tags:

--

Notes:

Nothing to report

RHEL-07-030800 (V-72183)

The Red Hat Enterprise Linux operating system must audit all uses of the crontab command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030800

Tags:

Notes:

Nothing to report

RHEL-07-030810 (V-72185)

The Red Hat Enterprise Linux operating system must audit all uses of the pam_timestamp_check command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Variables:

rhel_07_030810

Tags:

Notes:

Nothing to report

RHEL-07-030819 (V-78999)

The Red Hat Enterprise Linux operating system must audit all uses of the create_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030819

Tags:

Notes:

Nothing to report

RHEL-07-030820 (V-72187)

The Red Hat Enterprise Linux operating system must audit all uses of the init_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030820

Tags:

Notes:

Nothing to report

RHEL-07-030821 (V-79001)

The Red Hat Enterprise Linux operating system must audit all uses of the `finit_module` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030821

Tags:

Notes:

Nothing to report

RHEL-07-030830 (V-72189)

The Red Hat Enterprise Linux operating system must audit all uses of the `delete_module` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030830

Tags:

Notes:

Nothing to report

RHEL-07-030840 (V-72191)

The Red Hat Enterprise Linux operating system must audit all uses of the kmod command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030840

Tags:

--

Notes:

Nothing to report

RHEL-07-030870 (V-72197)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Variables:

rhel_07_030870

Tags:

--

Notes:

Nothing to report

RHEL-07-030871 (V-73165)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030871

Tags:

Notes:

Nothing to report

RHEL-07-030872 (V-73167)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030872

Tags:

Notes:

Nothing to report

RHEL-07-030873 (V-73171)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030873

Tags:

--

Notes:

Nothing to report

RHEL-07-030874 (V-73173)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030874

Tags:

--

Notes:

Nothing to report

RHEL-07-030880 (V-72199)

The Red Hat Enterprise Linux operating system must audit all uses of the rename syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030880

Tags:

Notes:

Nothing to report

RHEL-07-030890 (V-72201)

The Red Hat Enterprise Linux operating system must audit all uses of the renameat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030890

Tags:

Notes:

Nothing to report

RHEL-07-030900 (V-72203)

The Red Hat Enterprise Linux operating system must audit all uses of the rmdir syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030900

Tags:

Notes:

Nothing to report

RHEL-07-030910 (V-72205)

The Red Hat Enterprise Linux operating system must audit all uses of the unlink syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030910

Tags:

Notes:

Nothing to report

RHEL-07-030920 (V-72207)

The Red Hat Enterprise Linux operating system must audit all uses of the unlinkat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

```
rhel_07_030920
```

Tags:

Notes:

Nothing to report

RHEL-07-031000 (V-72209)

The Red Hat Enterprise Linux operating system must send rsyslog output to a log aggregation server.

Severity: Medium

Implementation Status: Implemented

Description:

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Variables:

```
rhel_07_031000
rhel7stig_log_aggregation_server is defined
```

Tags:

```
RHEL-07-031000
rsyslog
```

Notes:

Nothing to report

RHEL-07-031010 (V-72211)

The Red Hat Enterprise Linux operating system must be configured so that the rsyslog daemon does not accept log messages from other servers unless the server is being used for log aggregation.

Severity: Medium

Implementation Status: Implemented

Description:

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the system's logs, or could fill the system's storage leading to a Denial of Service.

If the system is intended to be a log aggregation server its use must be documented with the ISSO.

Variables:

```
rhel_07_031010
not rhel7stig_system_is_log_aggregator
```

Tags:

```
RHEL-07-031010
rsyslog
```

Notes:

Nothing to report

RHEL-07-040100 (V-72219)

The Red Hat Enterprise Linux operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.

Severity: Medium

Implementation Status: Not Implemented

Description:

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Variables:

```
rhel_07_040100
```

Tags:

```
RHEL-07-040100  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040110 (V-72221)

The Red Hat Enterprise Linux operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

Severity: Medium

Implementation Status: Implemented

Description:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Variables:

```
rhel_07_040110  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040110  
ssh
```

Notes:

Nothing to report

RHEL-07-040160 (V-72223)

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 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.

Severity: Medium**Implementation Status:** Implemented**Description:**

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Variables:

```
rhel_07_040160
```

Tags:

```
RHEL-07-040160
profile
```

Notes:

Nothing to report

RHEL-07-040170 (V-72225)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner immediately prior to, or as part of, remote access logon prompts.

Severity: Medium**Implementation Status:** Implemented**Description:**

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
```

(continues on next page)

(continued from previous page)

testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007 , SRG-OS-000228-GPOS-00088

Variables:

```
rhel_07_040170
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040170
ssh
dod_logon_banner
```

Notes:

Nothing to report

RHEL-07-040180 (V-72227)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_040180

Tags:

RHEL-07-040180
ldap
notimplemented

Notes:

Nothing to report

RHEL-07-040190 (V-72229)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_040190

Tags:

RHEL-07-040190
notimplemented

Notes:

Nothing to report

RHEL-07-040200 (V-72231)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

rhel_07_040200

Tags:

RHEL-07-040200 notimplemented

Notes:

Nothing to report

RHEL-07-040201 (V-77825)

The Red Hat Enterprise Linux operating system must implement virtual address space randomization.

Severity: Medium

Implementation Status: Implemented

Description:

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code he or she has introduced into a process's address space during an attempt at exploitation. Additionally, ASLR also makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return-oriented programming (ROP) techniques.

Variables:

rhel_07_040201

Tags:

RHEL-07-040201 sysctl

Notes:

Nothing to report

RHEL-07-040300 (V-72233)

The Red Hat Enterprise Linux operating system must be configured so that all networked systems have SSH installed.

Severity: Medium

Implementation Status: Implemented

Description:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Variables:

```
rhel_07_040300
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040300
ssh
```

Notes:

Nothing to report

RHEL-07-040310 (V-72235)

The Red Hat Enterprise Linux operating system must be configured so that all networked systems use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.

Severity: Medium

Implementation Status: Implemented

Description:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000423-GPOS-00188, SRG-OS-000423-GPOS-00189, SRG-OS-000423-GPOS-00190

Variables:

```
rhel_07_040310
rhel7stig_ssh_required
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
```

Tags:

```
RHEL-07-040310
ssh
```

Notes:

Nothing to report

RHEL-07-040320 (V-72237)

The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic are terminated at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Variables:

```
rhel_07_040320
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040320
ssh
```

Notes:

Nothing to report

RHEL-07-040330 (V-72239)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040330
rhel7stig_ssh_required
ansible_distribution_version is not version_compare('7.4', '>=')
```

Tags:

```
RHEL-07-040330
ssh
```

Notes:

Nothing to report

RHEL-07-040340 (V-72241)

The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic terminate after a period of inactivity.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Variables:

```
rhel_07_040340
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040340
ssh
```

Notes:

Nothing to report

RHEL-07-040350 (V-72243)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using rhosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040350
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040350
ssh
```

Notes:

Nothing to report

RHEL-07-040360 (V-72245)

The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon an SSH logon.

Severity: Medium

Implementation Status: Implemented

Description:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Variables:

```
rhel_07_040360
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040360
ssh
```

Notes:

Nothing to report

RHEL-07-040370 (V-72247)

The Red Hat Enterprise Linux operating system must not permit direct logons to the root account using remote access via SSH.

Severity: Medium

Implementation Status: Implemented

Description:

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Variables:

```
rhel_07_040370
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040370
ssh
```

Notes:

Nothing to report

RHEL-07-040380 (V-72249)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040380
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040380
ssh
```

Notes:

Nothing to report

RHEL-07-040400 (V-72253)

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.

Severity: Medium

Implementation Status: Implemented

Description:

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Variables:

```
rhel_07_040400
rhel7stig_ssh_required
```

Tags:

```
ssh
RHEL-07-040400
```

Notes:

Nothing to report

RHEL-07-040410 (V-72255)

The Red Hat Enterprise Linux operating system must be configured so that the SSH public host key files have mode 0644 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Variables:

```
rhel_07_040410
rhel7stig_ssh_required
```

Tags:


```
RHEL-07-040410
ssh
```

Notes:

Nothing to report

RHEL-07-040420 (V-72257)

The Red Hat Enterprise Linux operating system must be configured so that the SSH private host key files have mode 0640 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Variables:

```
rhel_07_040420
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040420
ssh
```

Notes:

Nothing to report

RHEL-07-040430 (V-72259)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Variables:

```
rhel_07_040430
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040430
ssh
```

Notes:

Nothing to report

RHEL-07-040440 (V-72261)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Variables:

```
rhel_07_040440
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040440
ssh
```

Notes:

Nothing to report

RHEL-07-040450 (V-72263)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon performs strict mode checking of home directory configuration files.

Severity: Medium

Implementation Status: Implemented

Description:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Variables:

```
rhel_07_040450
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040450
ssh
```

Notes:

Nothing to report

RHEL-07-040460 (V-72265)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon uses privilege separation.

Severity: Medium

Implementation Status: Implemented

Description:

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Variables:

```
rhel_07_040460
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040460
ssh
```

Notes:

Nothing to report

RHEL-07-040470 (V-72267)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.

Severity: Medium

Implementation Status: Implemented

Description:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Variables:

```
rhel_07_040470
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040470
ssh
```

Notes:

Nothing to report

RHEL-07-040500 (V-72269)

The Red Hat Enterprise Linux operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Severity: Medium

Implementation Status: Implemented

Description:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Variables:

```
rhel7stig_time_service == 'ntpd'
rhel_07_040500
rhel7stig_time_service == 'chronyd'
rhel_07_040500
rhel7stig_time_service == 'chronyd'
rhel_07_040500
```

Tags:

```
RHEL-07-040500
chronyd
```

Notes:

Nothing to report

RHEL-07-040510 (V-72271)

The Red Hat Enterprise Linux operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.

Severity: Medium

Implementation Status: Not Implemented

Description:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Variables:**Tags:****Notes:**

Nothing to report

RHEL-07-040520 (V-72273)

The Red Hat Enterprise Linux operating system must enable an application firewall, if available.

Severity: Medium

Implementation Status: Implemented

Description:

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Variables:

```
rhel_07_040520
rhel_07_040520
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
```

Tags:

```
RHEL-07-040520
firewall
```

Notes:

Nothing to report

RHEL-07-040610 (V-72283)

The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040610
```

Tags:

```
RHEL-07-040610  
ipv4
```

Notes:

Nothing to report

RHEL-07-040620 (V-72285)

The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040620
```

Tags:

`RHEL-07-040620`
`ipv4`

Notes:

Nothing to report

RHEL-07-040630 (V-72287)

The Red Hat Enterprise Linux operating system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

Severity: Medium

Implementation Status: Implemented

Description:

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Variables:

`rhel_07_040630`

Tags:

`RHEL-07-040630`
`ipv4`

Notes:

Nothing to report

RHEL-07-040640 (V-72289)

The Red Hat Enterprise Linux operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Variables:

`rhel_07_040640`

Tags:

```
RHEL-07-040640  
ipv4
```

Notes:

Nothing to report

RHEL-07-040641 (V-73175)

The Red Hat Enterprise Linux operating system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Variables:

```
rhel_07_040641
```

Tags:

```
RHEL-07-040641  
ipv4
```

Notes:

Nothing to report

RHEL-07-040650 (V-72291)

The Red Hat Enterprise Linux operating system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Variables:

```
rhel_07_040650
```

Tags:


```
RHEL-07-040650  
ipv4
```

Notes:

Nothing to report

RHEL-07-040660 (V-72293)

The Red Hat Enterprise Linux operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Variables:

```
rhel_07_040660
```

Tags:

```
RHEL-07-040660  
ipv4
```

Notes:

Nothing to report

RHEL-07-040670 (V-72295)

Network interfaces configured on the Red Hat Enterprise Linux operating system must not be in promiscuous mode.

Severity: Medium

Implementation Status: Implemented

Description:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Variables:

```
rhel_07_040670  
not rhel7stig_net_promisc_mode_required
```

Tags:

RHEL-07-040670

Notes:

Nothing to report

RHEL-07-040680 (V-72297)

The Red Hat Enterprise Linux operating system must be configured to prevent unrestricted mail relaying.

Severity: Medium

Implementation Status: Implemented

Description:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Variables:

rhel_07_040680

Tags:

RHEL-07-040680

Notes:

Nothing to report

RHEL-07-040720 (V-72305)

The Red Hat Enterprise Linux operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is configured to operate in secure mode.

Severity: Medium

Implementation Status: Implemented

Description:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Variables:

rhel7stig_tftp_required
rhel_07_040720

Tags:

RHEL-07-040720

Notes:

Nothing to report

RHEL-07-040730 (V-72307)

The Red Hat Enterprise Linux operating system must not have an X Windows display manager installed unless approved.

Severity: Medium

Implementation Status: Disruption High

Description:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Variables:

```
not rhel7stig_gui
rhel_07_040730
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040730
disruption-high
x11
gui
```

Notes:

Nothing to report

RHEL-07-040740 (V-72309)

The Red Hat Enterprise Linux operating system must not be performing packet forwarding unless the system is a router.

Severity: Medium

Implementation Status: Implemented

Description:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Variables:

```
not rhel7stig_system_is_router
rhel_07_040740
```

Tags:

```
RHEL-07-040740  
ipv4
```

Notes:

Nothing to report

RHEL-07-040750 (V-72311)

The Red Hat Enterprise Linux operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.

Severity: Medium

Implementation Status: Not Implemented

Description:

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Variables:

```
rhel_07_040750
```

Tags:

```
RHEL-07-040750  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040810 (V-72315)

The Red Hat Enterprise Linux operating system access control program must be configured to grant or deny system access to specific hosts and services.

Severity: Medium

Implementation Status: Not Implemented

Description:

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Variables:

`rhel_07_040810`

Tags:

`RHEL-07-040810`
`notimplemented`

Notes:

Nothing to report

RHEL-07-040820 (V-72317)

The Red Hat Enterprise Linux operating system must not have unauthorized IP tunnels configured.

Severity: Medium

Implementation Status: Disruption High

Description:

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the Information System Security Officer (ISSO).

Variables:

`rhel_07_040820`
`rhel7stig_disruptive`

Tags:

`RHEL-07-040820`
`disruption-high`

Notes:

Nothing to report

RHEL-07-040830 (V-72319)

The Red Hat Enterprise Linux operating system must not forward IPv6 source-routed packets.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Variables:

rhel_07_040830

Tags:

RHEL-07-040830
ipv6

Notes:

Nothing to report

RHEL-07-041001 (V-72417)

The Red Hat Enterprise Linux operating system must have the required packages for multifactor authentication installed.

Severity: Medium

Implementation Status: Implemented

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

rhel_07_041001

Tags:

RHEL-07-041001
multifactor

Notes:

Nothing to report

RHEL-07-041002 (V-72427)

The Red Hat Enterprise Linux operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

Severity: Medium

Implementation Status: Complexity High

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel7stig_auth_settings.use_sssd
rhel7stig_complex
rhel_07_041002
```

Tags:

```
RHEL-07-041002
complexity-high
sssd
```

Notes:

Nothing to report

RHEL-07-041003 (V-72433)

The Red Hat Enterprise Linux operating system must implement certificate status checking for PKI authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel_07_041003
ansible_distribution_major_version is version_compare('8', '<')
```

Tags:

```
RHEL-07-041003
```

Notes:

Nothing to report

RHEL-07-041010 (V-73177)

The Red Hat Enterprise Linux operating system must be configured so that all wireless network adapters are disabled.

Severity: Medium

Implementation Status: Implemented

Description:

The use of wireless networking can introduce many different attack vectors into the organization's network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial of service to valid network resources.

Variables:

```
rhel_07_041010
```

Tags:

```
RHEL-07-041010
```

Notes:

Nothing to report

Low (14 controls)**RHEL-07-020200 (V-71987)**

The Red Hat Enterprise Linux operating system must remove all software components after updated versions have been installed.

Severity: Low

Implementation Status: Implemented

Description:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Variables:

```
rhel_07_020200
```

Tags:

```
RHEL-07-020200
```

Notes:

Nothing to report

RHEL-07-020300 (V-72003)

The Red Hat Enterprise Linux operating system must be configured so that all Group Identifiers (GIDs) referenced in the `/etc/passwd` file are defined in the `/etc/group` file.

Severity: Low

Implementation Status: Complexity High

Description:

If a user is assigned the GID of a group not existing on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Variables:

```
rhel_07_020300  
rhel7stig_complex
```

Tags:

```
RHEL-07-020300  
complexity-high  
passwd
```

Notes:

Nothing to report

RHEL-07-021022 (V-81009)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the nodev option.

Severity: Low

Implementation Status: Implemented

Description:

The “nodev” mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021022 or rhel_07_021023 or rhel_07_021024
```

Tags:

```
RHEL-07-021022  
RHEL-07-021023  
RHEL-07-021024
```

Notes:

Nothing to report

RHEL-07-021023 (V-81011)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the nosuid option.

Severity: Low

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021022 or rhel_07_021023 or rhel_07_021024
```

Tags:

```
RHEL-07-021022  
RHEL-07-021023  
RHEL-07-021024
```

Notes:

Nothing to report

RHEL-07-021024 (V-81013)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the noexec option.

Severity: Low

Implementation Status: Implemented

Description:

The “noexec” mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021022 or rhel_07_021023 or rhel_07_021024
```

Tags:

```
RHEL-07-021022
RHEL-07-021023
RHEL-07-021024
```

Notes:

Nothing to report

RHEL-07-021310 (V-72059)

The Red Hat Enterprise Linux operating system must be configured so that a separate file system is used for user home directories (such as /home or an equivalent).

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021310
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/home$') | list | length == 0
```

Tags:

```
RHEL-07-021310
complexity-high
mount
home
```

Notes:

Nothing to report

RHEL-07-021320 (V-72061)

The Red Hat Enterprise Linux operating system must use a separate file system for /var.

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021320
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/var$') | list | length == 0
```

Tags:

```
RHEL-07-021320
complexity-high
mount
var
```

Notes:

Nothing to report

RHEL-07-021330 (V-72063)

The Red Hat Enterprise Linux operating system must use a separate file system for the system audit data path.

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021330
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/var/log/audit$') | list | length == 0
```

Tags:

```
RHEL-07-021330
complexity-high
mount
auditd
```

Notes:

Nothing to report

RHEL-07-021340 (V-72065)

The Red Hat Enterprise Linux operating system must use a separate file system for /tmp (or equivalent).

Severity: Low

Implementation Status: Implemented

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
rhel_07_021340
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
ansible_mounts | selectattr('mount', 'match', '^/tmp$') | list | length == 0
```

Tags:

```
RHEL-07-021340
mount
tmp
```

Notes:

Nothing to report

RHEL-07-021600 (V-72069)

The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).

Severity: Low

Implementation Status: Not Implemented

Description:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Variables:

rhel_07_021600

Tags:

RHEL-07-021600
notimplemented

Notes:

Nothing to report

RHEL-07-021610 (V-72071)

The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify extended attributes.

Severity: Low

Implementation Status: Not Implemented

Description:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Variables:

rhel_07_021610

Tags:

RHEL-07-021610
notimplemented

Notes:

Nothing to report

RHEL-07-040000 (V-72217)

The Red Hat Enterprise Linux operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

Severity: Low

Implementation Status: Implemented

Description:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Variables:

rhel_07_040000

Tags:

RHEL-07-040000

Notes:

Nothing to report

RHEL-07-040530 (V-72275)

The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon logon.

Severity: Low

Implementation Status: Implemented

Description:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Variables:

rhel_07_040530

Tags:

RHEL-07-040530
pamd

Notes:

Nothing to report

RHEL-07-040600 (V-72281)

For Red Hat Enterprise Linux operating systems using DNS resolution, at least two name servers must be configured.

Severity: Low

Implementation Status: Not Implemented

Description:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Variables:

rhel_07_040600

Tags:

RHEL-07-040600
notimplemented

Notes:

Nothing to report

Controls by Status

Contents

- *Controls by Status*
 - *Implemented (205 controls)*
 - *Complexity High (9 controls)*
 - *Disruption High (6 controls)*
 - *Not Implemented (23 controls)*

Implemented (205 controls)

RHEL-07-010010 (V-71849)

The Red Hat Enterprise Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.

Severity: High

Implementation Status: Implemented

Description:

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Variables:

rhel_07_010010

Tags:

RHEL-07-010010

Notes:

Nothing to report

RHEL-07-010020 (V-71855)

The Red Hat Enterprise Linux operating system must be configured so that the cryptographic hash of system files and commands matches vendor values.

Severity: High

Implementation Status: Implemented

Description:

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

```
rhel_07_010020
```

Tags:

```
RHEL-07-010020
```

Notes:

Nothing to report

RHEL-07-010030 (V-71859)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
```

(continues on next page)

(continued from previous page)

IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

```
rhel7stig_dconf_available  
rhel_07_010030  
rhel_07_010040
```

Tags:

```
RHEL-07-010030  
RHEL_07_010040  
dod_logon_banner  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010050 (V-71863)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Variables:

```
rhel_07_010050
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010050
ssh
dod_logon_banner
```

Notes:

Nothing to report

RHEL-07-010060 (V-71891)

The Red Hat Enterprise Linux operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures.

Severity: Medium

Implementation Status: Implemented

Description:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Variables:

```
rhel7stig_dconf_available  
rhel_07_010060
```

Tags:

```
RHEL-07-010060  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010061 (V-77819)

The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.

Severity: Medium

Implementation Status: Implemented

Description:

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Variables:

```
rhel7stig_dconf_available  
rhel_07_010061
```

Tags:

```
RHEL-07-010061
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010070 (V-71893)

The Red Hat Enterprise Linux operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available
rhel_07_010070
```

Tags:

```
RHEL-07-010070
dconf
gui
```

Notes:

Nothing to report

RHEL-07-010081 (V-73155)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver lock-delay setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence.

Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010081
```

Tags:

```
RHEL-07-010081  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010082 (V-73157)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010082
```

Tags:

```
RHEL-07-010082  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010090 (V-71897)

The Red Hat Enterprise Linux operating system must have the screen package installed.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The screen package allows for a session lock to be implemented and configured.

Variables:

```
rhel_07_010090
```

Tags:

```
RHEL-07-010090
```

Notes:

Nothing to report

RHEL-07-010100 (V-71899)

The Red Hat Enterprise Linux operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010100
```

Tags:

```
RHEL-07-010100  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010101 (V-78997)

The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

Severity: Medium

Implementation Status: Implemented

Description:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Variables:

```
rhel7stig_dconf_available  
rhel_07_010101
```

Tags:

```
RHEL-07-010101  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010110 (V-71901)

The Red Hat Enterprise Linux operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

Severity: Medium

Implementation Status: Implemented

Description:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Variables:


```
rhel7stig_dconf_available  
rhel_07_010110
```

Tags:

```
RHEL-07-010110  
dconf  
gui
```

Notes:

Nothing to report

RHEL-07-010119 (V-73159)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. “pwquality” enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

Variables:

```
rhel_07_010119
```

Tags:

```
RHEL-07-010119  
pamd
```

Notes:

Nothing to report

RHEL-07-010120 (V-71903)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one upper-case character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010120
```

Tags:

```
RHEL-07-010120  
pwquality
```

Notes:

Nothing to report

RHEL-07-010130 (V-71905)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one lower-case character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010130
```

Tags:

```
RHEL-07-010130  
pwquality
```

Notes:

Nothing to report

RHEL-07-010140 (V-71907)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010140
```

Tags:

```
RHEL-07-010140  
pwquality
```

Notes:

Nothing to report

RHEL-07-010150 (V-71909)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one special character.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

```
rhel_07_010150
```

Tags:

RHEL-07-010150 pwquality

Notes:

Nothing to report

RHEL-07-010160 (V-71911)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of eight of the total number of characters must be changed.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

rhel_07_010160

Tags:

RHEL-07-010160 pwquality

Notes:

Nothing to report

RHEL-07-010170 (V-71913)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of four character classes must be changed.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

rhel_07_010170

Tags:

RHEL-07-010170 pwquality

Notes:

Nothing to report

RHEL-07-010180 (V-71915)

The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed the number of repeating consecutive characters must not be more than three characters.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

rhel_07_010180

Tags:

RHEL-07-010180 pwquality

Notes:

Nothing to report

RHEL-07-010190 (V-71917)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Variables:

rhel_07_010190

Tags:

RHEL-07-010190 pwquality

Notes:

Nothing to report

RHEL-07-010200 (V-71919)

The Red Hat Enterprise Linux operating system must be configured so that the PAM system service is configured to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

rhel_07_010200

Tags:

RHEL-07-010200 pamd

Notes:

Nothing to report

RHEL-07-010210 (V-71921)

The Red Hat Enterprise Linux operating system must be configured to use the shadow file to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

```
rhel_07_010210
```

Tags:

```
RHEL-07-010210  
login
```

Notes:

Nothing to report

RHEL-07-010220 (V-71923)

The Red Hat Enterprise Linux operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

Severity: Medium

Implementation Status: Implemented

Description:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Variables:

```
rhel_07_010220
```

Tags:

```
RHEL-07-010220
```

Notes:

Nothing to report

RHEL-07-010230 (V-71925)

The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 24 hours/1 day minimum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Variables:

```
rhel_07_010230
```

Tags:

```
RHEL-07-010230  
login
```

Notes:

Nothing to report

RHEL-07-010240 (V-71927)

The Red Hat Enterprise Linux operating system must be configured so that passwords are restricted to a 24 hours/1 day minimum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Variables:

```
rhel_07_010240
```

Tags:

```
RHEL-07-010240  
password
```

Notes:

Nothing to report

RHEL-07-010250 (V-71929)

The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 60-day maximum lifetime.

Severity: Medium

Implementation Status: Implemented

Description:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Variables:

rhel_07_010250

Tags:

RHEL-07-010250 login

Notes:

Nothing to report

RHEL-07-010270 (V-71933)

The Red Hat Enterprise Linux operating system must be configured so that passwords are prohibited from reuse for a minimum of five generations.

Severity: Medium

Implementation Status: Implemented

Description:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Variables:

rhel_07_010270

Tags:

RHEL-07-010270 pamd

Notes:

Nothing to report

RHEL-07-010280 (V-71935)

The Red Hat Enterprise Linux operating system must be configured so that passwords are a minimum of 15 characters in length.

Severity: Medium

Implementation Status: Implemented

Description:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Variables:

```
rhel_07_010280
```

Tags:

```
RHEL-07-010280  
pwquality
```

Notes:

Nothing to report

RHEL-07-010290 (V-71937)

The Red Hat Enterprise Linux operating system must not have accounts configured with blank or null passwords.

Severity: High

Implementation Status: Implemented

Description:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Variables:

```
rhel_07_010290
```

Tags:

```
RHEL-07-010290  
pamd
```

Notes:

Nothing to report

RHEL-07-010300 (V-71939)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using an empty password.

Severity: High

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_010300
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010300
ssh
```

Notes:

Nothing to report

RHEL-07-010310 (V-71941)

The Red Hat Enterprise Linux operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

Severity: Medium

Implementation Status: Implemented

Description:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Variables:

```
rhel_07_010310
```

Tags:

```
RHEL-07-010310
```

Notes:

Nothing to report

RHEL-07-010320 (V-71943)

Accounts on the Red Hat Enterprise Linux operating system that are subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period.

Severity: Medium

Implementation Status: Implemented

Description:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Variables:

```
rhel_07_010320 or rhel_07_010330
```

Tags:

```
RHEL-07-010320  
RHEL-07-010330  
pamd
```

Notes:

Nothing to report

RHEL-07-010330 (V-71945)

The Red Hat Enterprise Linux operating system must lock the associated account after three unsuccessful root logon attempts are made within a 15-minute period.

Severity: Medium

Implementation Status: Implemented

Description:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Variables:

```
rhel_07_010320 or rhel_07_010330
```

Tags:

```
RHEL-07-010320  
RHEL-07-010330  
pamd
```

Notes:

Nothing to report

RHEL-07-010340 (V-71947)

The Red Hat Enterprise Linux operating system must be configured so that users must provide a password for privilege escalation.

Severity: Medium

Implementation Status: Implemented

Description:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Variables:

```
rhel7stig_using_password_auth  
rhel_07_010340
```

Tags:

```
RHEL-07-010340  
sudoers
```

Notes:

Nothing to report

RHEL-07-010350 (V-71949)

The Red Hat Enterprise Linux operating system must be configured so that users must re-authenticate for privilege escalation.

Severity: Medium

Implementation Status: Implemented

Description:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Variables:

```
rhel_07_010350
```

Tags:

```
RHEL-07-010350  
sudoers
```

Notes:

Nothing to report

RHEL-07-010430 (V-71951)

The Red Hat Enterprise Linux operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Variables:

```
rhel_07_010430
```

Tags:

```
RHEL-07-010430  
login
```

Notes:

Nothing to report

RHEL-07-010440 (V-71953)

The Red Hat Enterprise Linux operating system must not allow an unattended or automatic logon to the system via a graphical user interface.

Severity: High

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel7stig_gui  
rhel_07_010440
```

Tags:

```
RHEL-07-010440  
gui
```

Notes:

Nothing to report

RHEL-07-010450 (V-71955)

The Red Hat Enterprise Linux operating system must not allow an unrestricted logon to the system.

Severity: High

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel7stig_gui  
rhel_07_010450
```

Tags:

```
RHEL-07-010450  
gui
```

Notes:

Nothing to report

RHEL-07-010460 (V-71957)

The Red Hat Enterprise Linux operating system must not allow users to override SSH environment variables.

Severity: Medium

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel_07_010460  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010460  
ssh
```

Notes:

Nothing to report

RHEL-07-010470 (V-71959)

The Red Hat Enterprise Linux operating system must not allow a non-certificate trusted host SSH logon to the system.

Severity: Medium

Implementation Status: Implemented

Description:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Variables:

```
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-010470  
ssh
```

Notes:

Nothing to report

RHEL-07-010480 (V-71961)

Red Hat Enterprise Linux operating systems prior to version 7.2 with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010480 or rhel_07_010490  
ansible_distribution_version is version_compare('7.2', '<')
```

Tags:

```
RHEL-07-010480  
RHEL-07-010490  
grub  
bootloader
```


Notes:

Nothing to report

RHEL-07-010481 (V-77823)

The Red Hat Enterprise Linux operating system must require authentication upon booting into single-user and maintenance modes.

Severity: Medium

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Variables:

```
rhel_07_010481
```

Tags:

```
RHEL-07-010481  
rescue
```

Notes:

Nothing to report

RHEL-07-010482 (V-81005)

Red Hat Enterprise Linux operating systems version 7.2 or newer with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010482 or rhel_07_010491  
ansible_distribution_version is version_compare('7.2', '>=')
```

Tags:

```
RHEL-07-010482
RHEL-07-010491
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010490 (V-71963)

Red Hat Enterprise Linux operating systems prior to version 7.2 using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010480 or rhel_07_010490
ansible_distribution_version is version_compare('7.2', '<')
```

Tags:

```
RHEL-07-010480
RHEL-07-010490
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-010491 (V-81007)

Red Hat Enterprise Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Severity: High

Implementation Status: Implemented

Description:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is

the default boot loader for RHEL 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Variables:

```
rhel_07_010482 or rhel_07_010491
ansible_distribution_version is version_compare('7.2', '>=')
```

Tags:

```
RHEL-07-010482
RHEL-07-010491
grub
bootloader
```

Notes:

Nothing to report

RHEL-07-020000 (V-71967)

The Red Hat Enterprise Linux operating system must not have the rsh-server package installed.

Severity: High

Implementation Status: Implemented

Description:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Variables:

```
rhel_07_020000
```

Tags:

```
RHEL-07-020000
rsh
```

Notes:

Nothing to report

RHEL-07-020010 (V-71969)

The Red Hat Enterprise Linux operating system must not have the ypserv package installed.

Severity: High

Implementation Status: Implemented

Description:

Removing the “ypserv” package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Variables:

```
rhel_07_020010
```

Tags:

```
RHEL-07-020010  
ypserv
```

Notes:

Nothing to report

RHEL-07-020030 (V-71973)

The Red Hat Enterprise Linux operating system must be configured so that a file integrity tool verifies the baseline operating system configuration at least weekly.

Severity: Medium

Implementation Status: Implemented

Description:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system’s Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Variables:

```
rhel_07_020030 or rhel_07_020040
```

Tags:

```
RHEL-07-020030  
RHEL-07-020040  
aide
```

Notes:

Nothing to report

RHEL-07-020040 (V-71975)

The Red Hat Enterprise Linux operating system must be configured so that designated personnel are notified if baseline configurations are changed in an unauthorized manner.

Severity: Medium

Implementation Status: Implemented

Description:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's Information Management Officer (IMO)/Information System Security Officer (ISSO) and System Administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Variables:

```
rhel_07_020030 or rhel_07_020040
```

Tags:

```
RHEL-07-020030  
RHEL-07-020040  
aide
```

Notes:

Nothing to report

RHEL-07-020050 (V-71977)

The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Severity: High

Implementation Status: Implemented

Description:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Variables:

rhel_07_020050

Tags:

RHEL-07-020050
yum

Notes:

Nothing to report

RHEL-07-020060 (V-71979)

The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Severity: High

Implementation Status: Implemented

Description:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Variables:

rhel_07_020060

Tags:

RHEL-07-020060
yum

Notes:

Nothing to report

RHEL-07-020100 (V-71983)

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

Severity: Medium

Implementation Status: Implemented

Description:

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Variables:

rhel_07_020100

Tags:

RHEL-07-020100 usb_devices

Notes:

Nothing to report

RHEL-07-020101 (V-77821)

The Red Hat Enterprise Linux operating system must be configured so that the Datagram Congestion Control Protocol (DCCP) kernel module is disabled unless required.

Severity: Medium

Implementation Status: Implemented

Description:

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Variables:

rhel_07_020101

Tags:

RHEL-07-020101 dccp

Notes:

Nothing to report

RHEL-07-020110 (V-71985)

The Red Hat Enterprise Linux operating system must disable the file system automounter unless required.

Severity: Medium

Implementation Status: Implemented

Description:

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_020110
rhel_07_020110
rhel_07_020110_autofs_service_status.stdout == "loaded"
not rhel7stig_autofs_required
```

Tags:

```
RHEL-07-020110
```

Notes:

Nothing to report

RHEL-07-020200 (V-71987)

The Red Hat Enterprise Linux operating system must remove all software components after updated versions have been installed.

Severity: Low

Implementation Status: Implemented

Description:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Variables:

```
rhel_07_020200
```

Tags:

```
RHEL-07-020200
```

Notes:

Nothing to report

RHEL-07-020210 (V-71989)

The Red Hat Enterprise Linux operating system must enable SELinux.

Severity: High

Implementation Status: Implemented

Description:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Variables:

```
rhel_07_020210 or rhel_07_020220
not rhel7stig_system_is_container
```

Tags:

```
RHEL-07-020210
RHEL-07-020220
selinux
```

Notes:

Nothing to report

RHEL-07-020220 (V-71991)

The Red Hat Enterprise Linux operating system must enable the SELinux targeted policy.

Severity: High

Implementation Status: Implemented

Description:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Variables:

```
rhel_07_020210 or rhel_07_020220
not rhel7stig_system_is_container
```

Tags:

```
RHEL-07-020210
RHEL-07-020220
selinux
```

Notes:

Nothing to report

RHEL-07-020230 (V-71993)

The Red Hat Enterprise Linux operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled.

Severity: High

Implementation Status: Implemented

Description:

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Variables:

rhel_07_020230

Tags:

RHEL-07-020230

Notes:

Nothing to report

RHEL-07-020240 (V-71995)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Variables:

rhel_07_020240

Tags:

RHEL-07-020240
login
umask

Notes:

Nothing to report

RHEL-07-020260 (V-71999)

The Red Hat Enterprise Linux operating system security patches and updates must be installed and up to date.

Severity: Medium

Implementation Status: Implemented

Description:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Variables:

```
rhel_07_020260
rhel_07_020260
rhel_07_020260
rhel7stig_auto_package_updates_enabled or rhel_07_020260_yum_cron_installed.rc == 0
```

Tags:

```
RHEL-07-020260
packaging
```

Notes:

Nothing to report

RHEL-07-020270 (V-72001)

The Red Hat Enterprise Linux operating system must not have unnecessary accounts.

Severity: Medium

Implementation Status: Implemented

Description:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Variables:

```
rhel_07_020270
```

Tags:

```
RHEL-07-020270
```

Notes:

Nothing to report

RHEL-07-020310 (V-72005)

The Red Hat Enterprise Linux operating system must be configured so that the root account must be the only account having unrestricted access to the system.

Severity: High

Implementation Status: Implemented

Description:

If an account other than root also has a User Identifier (UID) of “0”, it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of “0” afford an opportunity for potential intruders to guess a password for a privileged account.

Variables:

rhel_07_020310

Tags:

RHEL-07-020310

Notes:

Nothing to report

RHEL-07-020600 (V-72011)

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.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Variables:

rhel_07_020600

Tags:

RHEL-07-020600

Notes:

Nothing to report

RHEL-07-020610 (V-72013)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Variables:

```
rhel_07_020610
```

Tags:

```
RHEL-07-020610  
login  
home
```

Notes:

Nothing to report

RHEL-07-020620 (V-72015)

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.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the `/` directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Variables:

```
rhel_07_020620  
item.uid >= 1000  
item.uid != 65534
```

Tags:

```
RHEL-07-020620
```

Notes:

Nothing to report

RHEL-07-020630 (V-72017)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories have mode 0750 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Variables:

```
rhel_07_020630
item.uid >= 1000
item.uid != 65534
```

Tags:

```
RHEL-07-020630
```

Notes:

Nothing to report

RHEL-07-020640 (V-72019)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are owned by their respective users.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user does not own their home directory, unauthorized users could access or modify the user's files, and the users may not be able to access their own files.

Variables:

```
rhel_07_020640
item.uid >= 1000
item.uid != 65534
```

Tags:

```
RHEL-07-020640
```

Notes:

Nothing to report

RHEL-07-020650 (V-72021)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners primary group.

Severity: Medium

Implementation Status: Implemented

Description:

If the Group Identifier (GID) of a local interactive user's home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

Variables:

```
rhel_07_020650
item.uid >= 1000
item.uid != 65534
```

Tags:

```
RHEL-07-020650
```

Notes:

Nothing to report

RHEL-07-020660 (V-72023)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are owned by the owner of the home directory.

Severity: Medium

Implementation Status: Implemented

Description:

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Variables:

```
rhel_07_020660
```

Tags:

```
RHEL-07-020660
```

Notes:

Nothing to report

RHEL-07-020670 (V-72025)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Variables:

rhel_07_020670

Tags:

RHEL-07-020670

Notes:

Nothing to report

RHEL-07-020680 (V-72027)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Variables:

rhel_07_020680

Tags:

RHEL-07-020680

Notes:

Nothing to report

RHEL-07-020690 (V-72029)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for interactive users are owned by the home directory user or root.

Severity: Medium

Implementation Status: Implemented

Description:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020690

Tags:

RHEL-07-020690

Notes:

Nothing to report

RHEL-07-020700 (V-72031)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for local interactive users are be group-owned by the users primary group or root.

Severity: Medium

Implementation Status: Implemented

Description:

Local initialization files for interactive users are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020700

Tags:

RHEL-07-020700

Notes:

Nothing to report

RHEL-07-021000 (V-72041)

The Red Hat Enterprise Linux operating system must be configured so that file systems containing user home directories are mounted to prevent files with the setuid and setgid bit set from being executed.

Severity: Medium

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute setuid and setgid files with owner privileges. This option must be used for mounting any file system not containing approved setuid and setgid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021000
ansible_mounts | selectattr('mount', 'match', '^/home$') | list | length != 0
'nosuid' not in home_mount.options
```

Tags:

```
RHEL-07-021000
```

Notes:

Nothing to report

RHEL-07-021020 (V-72045)

The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are being imported via Network File System (NFS).

Severity: Medium

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021020
'nosuid' not in (ansible_mounts | json_query(options_query))
```

Tags:

```
RHEL-07-021020
```

Notes:

Nothing to report

RHEL-07-021021 (V-73161)

The Red Hat Enterprise Linux operating system must prevent binary files from being executed on file systems that are being imported via Network File System (NFS).

Severity: Medium

Implementation Status: Implemented

Description:

The “noexec” mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021021
'noexec' not in (ansible_mounts | json_query(options_query))
```

Tags:

```
RHEL-07-021021
```

Notes:

Nothing to report

RHEL-07-021022 (V-81009)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the nodev option.

Severity: Low

Implementation Status: Implemented

Description:

The “nodev” mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021022 or rhel_07_021023 or rhel_07_021024
```

Tags:

```
RHEL-07-021022
RHEL-07-021023
RHEL-07-021024
```

Notes:

Nothing to report

RHEL-07-021023 (V-81011)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the nosuid option.

Severity: Low

Implementation Status: Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021022 or rhel_07_021023 or rhel_07_021024
```

Tags:

```
RHEL-07-021022  
RHEL-07-021023  
RHEL-07-021024
```

Notes:

Nothing to report

RHEL-07-021024 (V-81013)

The Red Hat Enterprise Linux operating system must mount /dev/shm with the noexec option.

Severity: Low

Implementation Status: Implemented

Description:

The “noexec” mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021022 or rhel_07_021023 or rhel_07_021024
```

Tags:

```
RHEL-07-021022  
RHEL-07-021023  
RHEL-07-021024
```

Notes:

Nothing to report

RHEL-07-021100 (V-72051)

The Red Hat Enterprise Linux operating system must have cron logging implemented.

Severity: Medium

Implementation Status: Implemented

Description:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Variables:

```
rhel_07_021100
```

Tags:

```
RHEL-07-021100
```

Notes:

Nothing to report

RHEL-07-021110 (V-72053)

The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is owned by root.

Severity: Medium

Implementation Status: Implemented

Description:

If the owner of the “cron.allow” file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Variables:

```
rhel_07_021110  
rhel_07_021120
```

Tags:

```
RHEL-07-021110  
RHEL-07-021120  
cron
```

Notes:

Nothing to report

RHEL-07-021120 (V-72055)

The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is group-owned by root.

Severity: Medium

Implementation Status: Implemented

Description:

If the group owner of the “cron.allow” file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Variables:

```
rhel_07_021110  
rhel_07_021120
```

Tags:

```
RHEL-07-021110  
RHEL-07-021120  
cron
```

Notes:

Nothing to report

RHEL-07-021300 (V-72057)

The Red Hat Enterprise Linux operating system must disable Kernel core dumps unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Variables:

```
rhel_07_021300
```

Tags:

```
RHEL-07-021300
```

Notes:

Nothing to report

RHEL-07-021340 (V-72065)

The Red Hat Enterprise Linux operating system must use a separate file system for /tmp (or equivalent).

Severity: Low

Implementation Status: Implemented

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
rhel_07_021340
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
ansible_mounts | selectattr('mount', 'match', '^/tmp$') | list | length == 0
```

Tags:

```
RHEL-07-021340
mount
tmp
```

Notes:

Nothing to report

RHEL-07-021350 (V-72067)

The Red Hat Enterprise Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Severity: High

Implementation Status: Implemented

Description:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Variables:

```
rhel_07_021350
ansible_distribution_major_version == '7'
```

Tags:

```
RHEL-07-021350
```

Notes:

Nothing to report

RHEL-07-021620 (V-72073)

The Red Hat Enterprise Linux operating system must use a file integrity tool that is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Severity: Medium

Implementation Status: Implemented

Description:

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Variables:

```
rhel_07_021620
```

Tags:

```
aide
RHEL-07-021620
```

Notes:

Nothing to report

RHEL-07-021710 (V-72077)

The Red Hat Enterprise Linux operating system must not have the telnet-server package installed.

Severity: High

Implementation Status: Implemented

Description:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Variables:

rhel_07_021710

Tags:

RHEL-07-021710
telnet

Notes:

Nothing to report

RHEL-07-030000 (V-72079)

The Red Hat Enterprise Linux operating system must be configured so that auditing is configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.

Severity: High

Implementation Status: Implemented

Description:

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096

Variables:

rhel_07_030000

Tags:

RHEL-07-030000
auditd

Notes:

Nothing to report

RHEL-07-030010 (V-72081)

The Red Hat Enterprise Linux operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.

Severity: Medium

Implementation Status: Implemented

Description:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Variables:

```
rhel_07_030010
```

Tags:

```
auditd  
RHEL-07-030010
```

Notes:

Nothing to report

RHEL-07-030200 (V-81015)

The Red Hat Enterprise Linux operating system must be configured to use the au-remote plugin.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the “au-remote” plugin, the audisp-remote daemon will not off-load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

`rhel_07_030200`

Tags:

`auditd`
`RHEL-07-030200`

Notes:

Nothing to report

RHEL-07-030300 (V-72083)

The Red Hat Enterprise Linux operating system must off-load audit records onto a different system or media from the system being audited.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

`rhel_07_030300` and `rhel7stig_audisp_remote_server`

Tags:

`auditd`
`RHEL-07-030300`

Notes:

Nothing to report

RHEL-07-030310 (V-72085)

The Red Hat Enterprise Linux operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

Severity: Medium

Implementation Status: Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

```
rhel_07_030310
```

Tags:

```
auditd  
RHEL-07-030310
```

Notes:

Nothing to report

RHEL-07-030320 (V-72087)

The Red Hat Enterprise Linux operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.

Severity: Medium

Implementation Status: Implemented

Description:

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Variables:

```
rhel_07_030320
```

Tags:

```
auditd  
RHEL-07-030320
```

Notes:

Nothing to report

RHEL-07-030321 (V-73163)

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.

Severity: Medium

Implementation Status: Implemented

Description:

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Variables:

`rhel_07_030321`

Tags:

`auditd`
`RHEL-07-030321`

Notes:

Nothing to report

RHEL-07-030330 (V-72089)

The Red Hat Enterprise Linux operating system must initiate an action to notify the System Administrator (SA) and Information System Security Officer ISSO, at a minimum, when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Variables:

`rhel_07_030330`

Tags:

`auditd`
`RHEL-07-030330`

Notes:

Nothing to report

RHEL-07-030340 (V-72091)

The Red Hat Enterprise Linux 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.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Variables:

rhel_07_030340

Tags:

auditd
RHEL-07-030340

Notes:

Nothing to report

RHEL-07-030350 (V-72093)

The Red Hat Enterprise Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Severity: Medium

Implementation Status: Implemented

Description:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Variables:

rhel_07_030350

Tags:

auditd
RHEL-07-030350

Notes:

Nothing to report

RHEL-07-030360 (V-72095)

The Red Hat Enterprise Linux operating system must audit all executions of privileged functions.

Severity: Medium

Implementation Status: Implemented

Description:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Variables:

`rhel_07_030360`

Tags:

`audit-rules`
`RHEL-07-030360`

Notes:

Nothing to report

RHEL-07-030370 (V-72097)

The Red Hat Enterprise Linux operating system must audit all uses of the `chown` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

`rhel_07_030370`

Tags:**Notes:**

Nothing to report

RHEL-07-030380 (V-72099)

The Red Hat Enterprise Linux operating system must audit all uses of the `fchown` syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030380

Tags:

--

Notes:

Nothing to report

RHEL-07-030390 (V-72101)

The Red Hat Enterprise Linux operating system must audit all uses of the lchown syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030390

Tags:

--

Notes:

Nothing to report

RHEL-07-030400 (V-72103)

The Red Hat Enterprise Linux operating system must audit all uses of the fchownat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Variables:

rhel_07_030400

Tags:

--

Notes:

Nothing to report

RHEL-07-030410 (V-72105)

The Red Hat Enterprise Linux operating system must audit all uses of the chmod syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030410

Tags:

--

Notes:

Nothing to report

RHEL-07-030420 (V-72107)

The Red Hat Enterprise Linux operating system must audit all uses of the fchmod syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030420

Tags:

Notes:

Nothing to report

RHEL-07-030430 (V-72109)

The Red Hat Enterprise Linux operating system must audit all uses of the fchmodat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030430

Tags:

Notes:

Nothing to report

RHEL-07-030440 (V-72111)

The Red Hat Enterprise Linux operating system must audit all uses of the setxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030440

Tags:

--

Notes:

Nothing to report

RHEL-07-030450 (V-72113)

The Red Hat Enterprise Linux operating system must audit all uses of the fsetxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030450

Tags:

--

Notes:

Nothing to report

RHEL-07-030460 (V-72115)

The Red Hat Enterprise Linux operating system must audit all uses of the lsetxattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030460

Tags:

--

Notes:

Nothing to report

RHEL-07-030470 (V-72117)

The Red Hat Enterprise Linux operating system must audit all uses of the removexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030470

Tags:

--

Notes:

Nothing to report

RHEL-07-030480 (V-72119)

The Red Hat Enterprise Linux operating system must audit all uses of the fremovexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030480

Tags:**Notes:**

Nothing to report

RHEL-07-030490 (V-72121)

The Red Hat Enterprise Linux operating system must audit all uses of the lremovexattr syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Variables:

rhel_07_030490

Tags:**Notes:**

Nothing to report

RHEL-07-030500 (V-72123)

The Red Hat Enterprise Linux operating system must audit all uses of the creat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030500
rhel_07_030500
```

Tags:

Notes:

Nothing to report

RHEL-07-030510 (V-72125)

The Red Hat Enterprise Linux operating system must audit all uses of the open syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030510
rhel_07_030510
```

Tags:

Notes:

Nothing to report

RHEL-07-030520 (V-72127)

The Red Hat Enterprise Linux operating system must audit all uses of the openat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030520
rhel_07_030520
```

Tags:**Notes:**

Nothing to report

RHEL-07-030530 (V-72129)

The Red Hat Enterprise Linux operating system must audit all uses of the open_by_handle_at syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030530
rhel_07_030530
```

Tags:

Notes:

Nothing to report

RHEL-07-030540 (V-72131)

The Red Hat Enterprise Linux operating system must audit all uses of the truncate syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030540
rhel_07_030540
```

Tags:**Notes:**

Nothing to report

RHEL-07-030550 (V-72133)

The Red Hat Enterprise Linux operating system must audit all uses of the ftruncate syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Variables:

```
rhel_07_030550
rhel_07_030550
```


Tags:**Notes:**

Nothing to report

RHEL-07-030560 (V-72135)

The Red Hat Enterprise Linux operating system must audit all uses of the semanage command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030560

Tags:**Notes:**

Nothing to report

RHEL-07-030570 (V-72137)

The Red Hat Enterprise Linux operating system must audit all uses of the setsebool command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030570

Tags:

Notes:

Nothing to report

RHEL-07-030580 (V-72139)

The Red Hat Enterprise Linux operating system must audit all uses of the chcon command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030580

Tags:

Notes:

Nothing to report

RHEL-07-030590 (V-72141)

The Red Hat Enterprise Linux operating system must audit all uses of the setfiles command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Variables:

rhel_07_030590

Tags:**Notes:**

Nothing to report

RHEL-07-030610 (V-72145)

The Red Hat Enterprise Linux operating system must generate audit records for all unsuccessful account access events.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Variables:

rhel_07_030610

Tags:**Notes:**

Nothing to report

RHEL-07-030620 (V-72147)

The Red Hat Enterprise Linux operating system must generate audit records for all successful account access events.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Variables:

rhel_07_030620

Tags:**Notes:**

Nothing to report

RHEL-07-030630 (V-72149)

The Red Hat Enterprise Linux operating system must audit all uses of the passwd command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030630

Tags:**Notes:**

Nothing to report

RHEL-07-030640 (V-72151)

The Red Hat Enterprise Linux operating system must audit all uses of the unix_chkpwd command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030640

Tags:

--

Notes:

Nothing to report

RHEL-07-030650 (V-72153)

The Red Hat Enterprise Linux operating system must audit all uses of the gpasswd command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030650

Tags:

--

Notes:

Nothing to report

RHEL-07-030660 (V-72155)

The Red Hat Enterprise Linux operating system must audit all uses of the chage command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030660

Tags:

--

Notes:

Nothing to report

RHEL-07-030670 (V-72157)

The Red Hat Enterprise Linux operating system must audit all uses of the userhelper command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030670

Tags:

--

Notes:

Nothing to report

RHEL-07-030680 (V-72159)

The Red Hat Enterprise Linux operating system must audit all uses of the su command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030680

Tags:**Notes:**

Nothing to report

RHEL-07-030690 (V-72161)

The Red Hat Enterprise Linux operating system must audit all uses of the sudo command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030690

Tags:**Notes:**

Nothing to report

RHEL-07-030700 (V-72163)

The Red Hat Enterprise Linux operating system must audit all uses of the sudoers file and all files in the /etc/sudoers.d/ directory.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

```
rhel_07_030700
rhel_07_030700
```

Tags:

Notes:

Nothing to report

RHEL-07-030710 (V-72165)

The Red Hat Enterprise Linux operating system must audit all uses of the newgrp command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

```
rhel_07_030710
```

Tags:

Notes:

Nothing to report

RHEL-07-030720 (V-72167)

The Red Hat Enterprise Linux operating system must audit all uses of the chsh command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030720

Tags:**Notes:**

Nothing to report

RHEL-07-030740 (V-72171)

The Red Hat Enterprise Linux operating system must audit all uses of the mount command and syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030740

Tags:**Notes:**

Nothing to report

RHEL-07-030750 (V-72173)

The Red Hat Enterprise Linux operating system must audit all uses of the umount command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030750

Tags:**Notes:**

Nothing to report

RHEL-07-030760 (V-72175)

The Red Hat Enterprise Linux operating system must audit all uses of the postdrop command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030760

Tags:**Notes:**

Nothing to report

RHEL-07-030770 (V-72177)

The Red Hat Enterprise Linux operating system must audit all uses of the postqueue command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Variables:

rhel_07_030770

Tags:**Notes:**

Nothing to report

RHEL-07-030780 (V-72179)

The Red Hat Enterprise Linux operating system must audit all uses of the ssh-keysign command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030780

Tags:

--

Notes:

Nothing to report

RHEL-07-030800 (V-72183)

The Red Hat Enterprise Linux operating system must audit all uses of the crontab command.

Severity: Medium

Implementation Status: Implemented

Description:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Variables:

rhel_07_030800

Tags:

--

Notes:

Nothing to report

RHEL-07-030810 (V-72185)

The Red Hat Enterprise Linux operating system must audit all uses of the pam_timestamp_check command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Variables:

rhel_07_030810

Tags:**Notes:**

Nothing to report

RHEL-07-030819 (V-78999)

The Red Hat Enterprise Linux operating system must audit all uses of the create_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030819

Tags:**Notes:**

Nothing to report

RHEL-07-030820 (V-72187)

The Red Hat Enterprise Linux operating system must audit all uses of the init_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030820

Tags:

--

Notes:

Nothing to report

RHEL-07-030821 (V-79001)

The Red Hat Enterprise Linux operating system must audit all uses of the finit_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030821

Tags:

--

Notes:

Nothing to report

RHEL-07-030830 (V-72189)

The Red Hat Enterprise Linux operating system must audit all uses of the delete_module syscall.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030830

Tags:

--

Notes:

Nothing to report

RHEL-07-030840 (V-72191)

The Red Hat Enterprise Linux operating system must audit all uses of the kmod command.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Variables:

rhel_07_030840

Tags:

--

Notes:

Nothing to report

RHEL-07-030870 (V-72197)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Variables:

rhel_07_030870

Tags:

Notes:

Nothing to report

RHEL-07-030871 (V-73165)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030871

Tags:

Notes:

Nothing to report

RHEL-07-030872 (V-73167)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030872

Tags:

--

Notes:

Nothing to report

RHEL-07-030873 (V-73171)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030873

Tags:

--

Notes:

Nothing to report

RHEL-07-030874 (V-73173)

The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

Severity: Medium

Implementation Status: Implemented

Description:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Variables:

rhel_07_030874

Tags:

--

Notes:

Nothing to report

RHEL-07-030880 (V-72199)

The Red Hat Enterprise Linux operating system must audit all uses of the rename syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030880

Tags:

--

Notes:

Nothing to report

RHEL-07-030890 (V-72201)

The Red Hat Enterprise Linux operating system must audit all uses of the renameat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030890

Tags:

Notes:

Nothing to report

RHEL-07-030900 (V-72203)

The Red Hat Enterprise Linux operating system must audit all uses of the rmdir syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030900

Tags:

Notes:

Nothing to report

RHEL-07-030910 (V-72205)

The Red Hat Enterprise Linux operating system must audit all uses of the unlink syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

rhel_07_030910

Tags:

Notes:

Nothing to report

RHEL-07-030920 (V-72207)

The Red Hat Enterprise Linux operating system must audit all uses of the unlinkat syscall.

Severity: Medium

Implementation Status: Implemented

Description:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Variables:

`rhel_07_030920`

Tags:**Notes:**

Nothing to report

RHEL-07-031000 (V-72209)

The Red Hat Enterprise Linux operating system must send rsyslog output to a log aggregation server.

Severity: Medium

Implementation Status: Implemented

Description:

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Variables:

`rhel_07_031000`
`rhel7stig_log_aggregation_server` is defined

Tags:

`RHEL-07-031000`
`rsyslog`

Notes:

Nothing to report

RHEL-07-031010 (V-72211)

The Red Hat Enterprise Linux operating system must be configured so that the rsyslog daemon does not accept log messages from other servers unless the server is being used for log aggregation.

Severity: Medium

Implementation Status: Implemented

Description:

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the system's logs, or could fill the system's storage leading to a Denial of Service.

If the system is intended to be a log aggregation server its use must be documented with the ISSO.

Variables:

```
rhel_07_031010
not rhel7stig_system_is_log_aggregator
```

Tags:

```
RHEL-07-031010
rsyslog
```

Notes:

Nothing to report

RHEL-07-032000 (V-72213)

The Red Hat Enterprise Linux operating system must use a virus scan program.

Severity: High

Implementation Status: Implemented

Description:

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Variables:

```
rhel7stig_antivirus_required  
rhel_07_032000
```

Tags:

```
RHEL-07-032000  
antivirus
```

Notes:

Nothing to report

RHEL-07-040000 (V-72217)

The Red Hat Enterprise Linux operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

Severity: Low

Implementation Status: Implemented

Description:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Variables:

```
rhel_07_040000
```

Tags:

```
RHEL-07-040000
```

Notes:

Nothing to report

RHEL-07-040110 (V-72221)

The Red Hat Enterprise Linux operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

Severity: Medium

Implementation Status: Implemented

Description:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Variables:

```
rhel_07_040110
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040110
ssh
```

Notes:

Nothing to report

RHEL-07-040160 (V-72223)

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 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Variables:

```
rhel_07_040160
```

Tags:

```
RHEL-07-040160
profile
```

Notes:

Nothing to report

RHEL-07-040170 (V-72225)

The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner immediately prior to, or as part of, remote access logon prompts.

Severity: Medium

Implementation Status: Implemented

Description:

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007 , SRG-OS-000228-GPOS-00088

Variables:

```
rhel_07_040170
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040170
ssh
dod_logon_banner
```

Notes:

Nothing to report

RHEL-07-040201 (V-77825)

The Red Hat Enterprise Linux operating system must implement virtual address space randomization.

Severity: Medium

Implementation Status: Implemented

Description:

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code he or she has introduced into a process's address space during an attempt at exploitation. Additionally, ASLR also makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return-oriented programming (ROP) techniques.

Variables:

```
rhel_07_040201
```

Tags:

```
RHEL-07-040201
sysctl
```

Notes:

Nothing to report

RHEL-07-040300 (V-72233)

The Red Hat Enterprise Linux operating system must be configured so that all networked systems have SSH installed.

Severity: Medium

Implementation Status: Implemented

Description:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Variables:

```
rhel_07_040300
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040300
ssh
```

Notes:

Nothing to report

RHEL-07-040310 (V-72235)

The Red Hat Enterprise Linux operating system must be configured so that all networked systems use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.

Severity: Medium

Implementation Status: Implemented

Description:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000423-GPOS-00188, SRG-OS-000423-GPOS-00189, SRG-OS-000423-GPOS-00190

Variables:

```
rhel_07_040310
rhel7stig_ssh_required
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
```

Tags:

`RHEL-07-040310`
`ssh`

Notes:

Nothing to report

RHEL-07-040320 (V-72237)

The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic are terminated at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Variables:

`rhel_07_040320`
`rhel7stig_ssh_required`

Tags:

`RHEL-07-040320`
`ssh`

Notes:

Nothing to report

RHEL-07-040330 (V-72239)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040330
rhel7stig_ssh_required
ansible_distribution_version is not version_compare('7.4', '>=')
```

Tags:

```
RHEL-07-040330
ssh
```

Notes:

Nothing to report

RHEL-07-040340 (V-72241)

The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic terminate after a period of inactivity.

Severity: Medium

Implementation Status: Implemented

Description:

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Variables:

```
rhel_07_040340
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040340
ssh
```

Notes:

Nothing to report

RHEL-07-040350 (V-72243)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using rhosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040350
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040350
ssh
```

Notes:

Nothing to report

RHEL-07-040360 (V-72245)

The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon an SSH logon.

Severity: Medium

Implementation Status: Implemented

Description:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Variables:

```
rhel_07_040360
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040360
ssh
```

Notes:

Nothing to report

RHEL-07-040370 (V-72247)

The Red Hat Enterprise Linux operating system must not permit direct logons to the root account using remote access via SSH.

Severity: Medium

Implementation Status: Implemented

Description:

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Variables:

```
rhel_07_040370
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040370
ssh
```

Notes:

Nothing to report

RHEL-07-040380 (V-72249)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Variables:

```
rhel_07_040380
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040380
ssh
```

Notes:

Nothing to report

RHEL-07-040390 (V-72251)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon is configured to only use the SSHv2 protocol.

Severity: High

Implementation Status: Implemented

Description:

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Variables:

```
rhel_07_040390
rhel7stig_ssh_required
ansible_distribution_version is not version_compare('7.4', '>=')
```

Tags:

```
RHEL-07-040390
ssh
```

Notes:

Nothing to report

RHEL-07-040400 (V-72253)

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.

Severity: Medium

Implementation Status: Implemented

Description:

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Variables:

```
rhel_07_040400  
rhel7stig_ssh_required
```

Tags:

```
ssh  
RHEL-07-040400
```

Notes:

Nothing to report

RHEL-07-040410 (V-72255)

The Red Hat Enterprise Linux operating system must be configured so that the SSH public host key files have mode 0644 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Variables:

```
rhel_07_040410  
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040410  
ssh
```

Notes:

Nothing to report

RHEL-07-040420 (V-72257)

The Red Hat Enterprise Linux operating system must be configured so that the SSH private host key files have mode 0640 or less permissive.

Severity: Medium

Implementation Status: Implemented

Description:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Variables:


```
rhel_07_040420
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040420
ssh
```

Notes:

Nothing to report

RHEL-07-040430 (V-72259)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Variables:

```
rhel_07_040430
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040430
ssh
```

Notes:

Nothing to report

RHEL-07-040440 (V-72261)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.

Severity: Medium

Implementation Status: Implemented

Description:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos

implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Variables:

```
rhel_07_040440
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040440
ssh
```

Notes:

Nothing to report

RHEL-07-040450 (V-72263)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon performs strict mode checking of home directory configuration files.

Severity: Medium

Implementation Status: Implemented

Description:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Variables:

```
rhel_07_040450
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040450
ssh
```

Notes:

Nothing to report

RHEL-07-040460 (V-72265)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon uses privilege separation.

Severity: Medium

Implementation Status: Implemented

Description:

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Variables:

```
rhel_07_040460
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040460
ssh
```

Notes:

Nothing to report

RHEL-07-040470 (V-72267)

The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.

Severity: Medium

Implementation Status: Implemented

Description:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Variables:

```
rhel_07_040470
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040470
ssh
```

Notes:

Nothing to report

RHEL-07-040500 (V-72269)

The Red Hat Enterprise Linux operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Severity: Medium

Implementation Status: Implemented

Description:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Variables:

```
rhel7stig_time_service == 'ntpd'
rhel_07_040500
rhel7stig_time_service == 'chronyd'
rhel_07_040500
rhel7stig_time_service == 'chronyd'
rhel_07_040500
```

Tags:

```
RHEL-07-040500
chronyd
```

Notes:

Nothing to report

RHEL-07-040520 (V-72273)

The Red Hat Enterprise Linux operating system must enable an application firewall, if available.

Severity: Medium

Implementation Status: Implemented

Description:

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Variables:

```
rhel_07_040520
rhel_07_040520
not (rhel7stig_system_is_chroot and rhel7stig_system_is_container)
```

Tags:

```
RHEL-07-040520
firewall
```

Notes:

Nothing to report

RHEL-07-040530 (V-72275)

The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon logon.

Severity: Low

Implementation Status: Implemented

Description:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Variables:

rhel_07_040530

Tags:

RHEL-07-040530 pamd

Notes:

Nothing to report

RHEL-07-040540 (V-72277)

The Red Hat Enterprise Linux operating system must not contain .shosts files.

Severity: High

Implementation Status: Implemented

Description:

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Variables:

rhel_07_040540

Tags:

RHEL-07-040540 shosts

Notes:

Nothing to report

RHEL-07-040550 (V-72279)

The Red Hat Enterprise Linux operating system must not contain shosts.equiv files.

Severity: High

Implementation Status: Implemented

Description:

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Variables:

```
rhel_07_040550
```

Tags:

```
RHEL-07-040550  
shosts
```

Notes:

Nothing to report

RHEL-07-040610 (V-72283)

The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040610
```

Tags:

```
RHEL-07-040610  
ipv4
```

Notes:

Nothing to report

RHEL-07-040620 (V-72285)

The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Variables:

rhel_07_040620

Tags:

RHEL-07-040620
ipv4

Notes:

Nothing to report

RHEL-07-040630 (V-72287)

The Red Hat Enterprise Linux operating system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

Severity: Medium

Implementation Status: Implemented

Description:

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Variables:

rhel_07_040630

Tags:

RHEL-07-040630
ipv4

Notes:

Nothing to report

RHEL-07-040640 (V-72289)

The Red Hat Enterprise Linux operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Variables:

```
rhel_07_040640
```

Tags:

```
RHEL-07-040640  
ipv4
```

Notes:

Nothing to report

RHEL-07-040641 (V-73175)

The Red Hat Enterprise Linux operating system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Variables:

```
rhel_07_040641
```

Tags:

```
RHEL-07-040641  
ipv4
```

Notes:

Nothing to report

RHEL-07-040650 (V-72291)

The Red Hat Enterprise Linux operating system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Variables:

rhel_07_040650

Tags:

RHEL-07-040650 ipv4

Notes:

Nothing to report

RHEL-07-040660 (V-72293)

The Red Hat Enterprise Linux operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.

Severity: Medium

Implementation Status: Implemented

Description:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Variables:

rhel_07_040660

Tags:

RHEL-07-040660 ipv4

Notes:

Nothing to report

RHEL-07-040670 (V-72295)

Network interfaces configured on the Red Hat Enterprise Linux operating system must not be in promiscuous mode.

Severity: Medium

Implementation Status: Implemented

Description:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Variables:

```
rhel_07_040670
not rhel7stig_net_promisc_mode_required
```

Tags:

```
RHEL-07-040670
```

Notes:

Nothing to report

RHEL-07-040680 (V-72297)

The Red Hat Enterprise Linux operating system must be configured to prevent unrestricted mail relaying.

Severity: Medium

Implementation Status: Implemented

Description:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Variables:

```
rhel_07_040680
```

Tags:

```
RHEL-07-040680
```

Notes:

Nothing to report

RHEL-07-040710 (V-72303)

The Red Hat Enterprise Linux operating system must be configured so that remote X connections for interactive users are encrypted.

Severity: High

Implementation Status: Implemented

Description:

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Variables:

```
rhel_07_040710
rhel7stig_ssh_required
```

Tags:

```
RHEL-07-040710
ssh
```

Notes:

Nothing to report

RHEL-07-040720 (V-72305)

The Red Hat Enterprise Linux operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is configured to operate in secure mode.

Severity: Medium

Implementation Status: Implemented

Description:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Variables:

```
rhel7stig_tftp_required
rhel_07_040720
```

Tags:

```
RHEL-07-040720
```

Notes:

Nothing to report

RHEL-07-040740 (V-72309)

The Red Hat Enterprise Linux operating system must not be performing packet forwarding unless the system is a router.

Severity: Medium

Implementation Status: Implemented

Description:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Variables:

```
not rhel7stig_system_is_router
rhel_07_040740
```

Tags:

```
RHEL-07-040740
ipv4
```

Notes:

Nothing to report

RHEL-07-040800 (V-72313)

SNMP community strings on the Red Hat Enterprise Linux operating system must be changed from the default.

Severity: High

Implementation Status: Implemented

Description:

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Variables:

```
rhel_07_040800
```

Tags:

```
RHEL-07-040800
snmp
```

Notes:

Nothing to report

RHEL-07-040830 (V-72319)

The Red Hat Enterprise Linux operating system must not forward IPv6 source-routed packets.

Severity: Medium

Implementation Status: Implemented

Description:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Variables:

```
rhel_07_040830
```

Tags:

```
RHEL-07-040830  
ipv6
```

Notes:

Nothing to report

RHEL-07-041001 (V-72417)

The Red Hat Enterprise Linux operating system must have the required packages for multifactor authentication installed.

Severity: Medium

Implementation Status: Implemented

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel_07_041001
```

Tags:

```
RHEL-07-041001  
multifactor
```

Notes:

Nothing to report

RHEL-07-041003 (V-72433)

The Red Hat Enterprise Linux operating system must implement certificate status checking for PKI authentication.

Severity: Medium

Implementation Status: Implemented

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel_07_041003  
ansible_distribution_major_version is version_compare('8', '<')
```

Tags:

```
RHEL-07-041003
```

Notes:

Nothing to report

RHEL-07-041010 (V-73177)

The Red Hat Enterprise Linux operating system must be configured so that all wireless network adapters are disabled.

Severity: Medium

Implementation Status: Implemented

Description:

The use of wireless networking can introduce many different attack vectors into the organization's network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial of service to valid network resources.

Variables:

```
rhel_07_041010
```

Tags:

```
RHEL-07-041010
```

Notes:

Nothing to report

Complexity High (9 controls)**RHEL-07-020250 (V-71997)**

The Red Hat Enterprise Linux operating system must be a vendor supported release.

Severity: High

Implementation Status: Complexity High

Description:

An operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Variables:

```
rhel_07_020250  
rhel7stig_complex
```

Tags:

```
RHEL-07-020250  
complexity-high
```

Notes:

Nothing to report

RHEL-07-020300 (V-72003)

The Red Hat Enterprise Linux operating system must be configured so that all Group Identifiers (GIDs) referenced in the `/etc/passwd` file are defined in the `/etc/group` file.

Severity: Low

Implementation Status: Complexity High

Description:

If a user is assigned the GID of a group not existing on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Variables:

```
rhel_07_020300
rhel7stig_complex
```

Tags:

```
RHEL-07-020300
complexity-high
passwd
```

Notes:

Nothing to report

RHEL-07-020320 (V-72007)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid owner.

Severity: Medium

Implementation Status: Complexity High

Description:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier “UID” as the UID of the un-owned files.

Variables:

```
rhel_07_020320
rhel7stig_complex
```

Tags:

```
RHEL-07-020320
complexity-high
```

Notes:

Nothing to report

RHEL-07-020330 (V-72009)

The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid group owner.

Severity: Medium

Implementation Status: Complexity High

Description:

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Variables:

```
rhel_07_020330
rhel7stig_complex
```

Tags:

```
RHEL-07-020330
complexity-high
```

Notes:

Nothing to report

RHEL-07-020900 (V-72039)

The Red Hat Enterprise Linux operating system must be configured so that all system device files are correctly labeled to prevent unauthorized modification.

Severity: Medium

Implementation Status: Complexity High

Description:

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Variables:

```
rhel_07_020900
rhel7stig_complex
ansible_selinux is not defined
rhel_07_020900
rhel7stig_complex
ansible_selinux.status == "enabled"
```

Tags:

```
RHEL-07-020900
complexity-high
```

Notes:

Nothing to report

RHEL-07-021310 (V-72059)

The Red Hat Enterprise Linux operating system must be configured so that a separate file system is used for user home directories (such as /home or an equivalent).

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021310
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/home$') | list | length == 0
```

Tags:

```
RHEL-07-021310
complexity-high
mount
home
```

Notes:

Nothing to report

RHEL-07-021320 (V-72061)

The Red Hat Enterprise Linux operating system must use a separate file system for /var.

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021320
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/var$') | list | length == 0
```

Tags:

```
RHEL-07-021320
complexity-high
mount
var
```

Notes:

Nothing to report

RHEL-07-021330 (V-72063)

The Red Hat Enterprise Linux operating system must use a separate file system for the system audit data path.

Severity: Low

Implementation Status: Complexity High

Description:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Variables:

```
not rhel7stig_system_is_container
rhel_07_021330
rhel7stig_complex
ansible_mounts | selectattr('mount', 'match', '^/var/log/audit$') | list | length == 0
```

Tags:

```
RHEL-07-021330
complexity-high
mount
auditd
```

Notes:

Nothing to report

RHEL-07-041002 (V-72427)

The Red Hat Enterprise Linux operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

Severity: Medium

Implementation Status: Complexity High

Description:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000375-GPOS-00161, SRG-OS-000375-GPOS-00162

Variables:

```
rhel7stig_auth_settings.use_sssd
rhel7stig_complex
rhel_07_041002
```

Tags:

```
RHEL-07-041002
complexity-high
sssd
```

Notes:

Nothing to report

Disruption High (6 controls)

RHEL-07-010260 (V-71931)

The Red Hat Enterprise Linux operating system must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

Severity: Medium

Implementation Status: Disruption High

Description:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Variables:

```
rhel_07_010260
rhel7stig_disruptive
```

Tags:

```
RHEL-07-010260
disruption-high
password
```

Notes:

Nothing to report

RHEL-07-021030 (V-72047)

The Red Hat Enterprise Linux operating system must be configured so that all world-writable directories are group-owned by root, sys, bin, or an application group.

Severity: Medium

Implementation Status: Disruption High

Description:

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Variables:

```
rhel_07_021030
rhel7stig_disruptive
```

Tags:

```
RHEL-07-021030
disruption-high
```

Notes:

Nothing to report

RHEL-07-040690 (V-72299)

The Red Hat Enterprise Linux operating system must not have a File Transfer Protocol (FTP) server package installed unless needed.

Severity: High

Implementation Status: Disruption High

Description:

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Variables:

```
not rhel7stig_vsftpd_required
rhel_07_040690
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040690
disruption-high
ftp
```

Notes:

Nothing to report

RHEL-07-040700 (V-72301)

The Red Hat Enterprise Linux operating system must not have the Trivial File Transfer Protocol (TFTP) server package installed if not required for operational support.

Severity: High

Implementation Status: Disruption High

Description:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Variables:

```
not rhel7stig_tftp_required
rhel_07_040700
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040700
disruption-high
tftp
```

Notes:

Nothing to report

RHEL-07-040730 (V-72307)

The Red Hat Enterprise Linux operating system must not have an X Windows display manager installed unless approved.

Severity: Medium

Implementation Status: Disruption High

Description:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Variables:

```
not rhel7stig_gui  
rhel_07_040730  
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040730  
disruption-high  
x11  
gui
```

Notes:

Nothing to report

RHEL-07-040820 (V-72317)

The Red Hat Enterprise Linux operating system must not have unauthorized IP tunnels configured.

Severity: Medium

Implementation Status: Disruption High

Description:

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the Information System Security Officer (ISSO).

Variables:

```
rhel_07_040820  
rhel7stig_disruptive
```

Tags:

```
RHEL-07-040820  
disruption-high
```

Notes:

Nothing to report

Not Implemented (23 controls)**RHEL-07-010040 (V-71861)**

The Red Hat Enterprise Linux operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user login.

Severity: Medium

Implementation Status: Not Implemented

Description:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
You are accessing a U.S. Government (USG) Information System (IS)
that is provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS),
you consent to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration
testing, COMSEC monitoring, network operations and defense,
personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this
IS.
```

```
-Communications using, or data stored on, this IS are not private,
are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal
benefit or privacy.
```

```
-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of
the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential. See
User Agreement for details.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Variables:

Tags:

Notes:

Nothing to report

RHEL-07-010118 (V-81003)

The Red Hat Enterprise Linux operating system must be configured so that /etc/pam.d/passwd implements /etc/pam.d/system-auth when changing passwords.

Severity: Medium

Implementation Status: Not Implemented

Description:

Pluggable authentication modules (PAM) allow for a modular approach to integrating authentication methods. PAM operates in a top-down processing model and if the modules are not listed in the correct order, an important security function could be bypassed if stack entries are not centralized.

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-010500 (V-71965)

The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.

Severity: Medium

Implementation Status: Not Implemented

Description:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

- 1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication;

and

- 2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Variables:

```
rhel_07_010500
```

Tags:

```
RHEL-07-010500  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020020 (V-71971)

The Red Hat Enterprise Linux operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Severity: Medium

Implementation Status: Not Implemented

Description:

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Variables:

```
rhel_07_020020
```

Tags:

```
RHEL-07-020020  
notimplemented
```

Notes:

Nothing to report

RHEL-07-020710 (V-72033)

The Red Hat Enterprise Linux operating system must be configured so that all local initialization files have mode 0740 or less permissive.

Severity: Medium

Implementation Status: Not Implemented

Description:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Variables:

rhel_07_020710

Tags:

RHEL-07-020710 notimplemented

Notes:

Nothing to report

RHEL-07-020720 (V-72035)

The Red Hat Enterprise Linux operating system must be configured so that all local interactive user initialization files executable search paths contain only paths that resolve to the users home directory.

Severity: Medium

Implementation Status: Not Implemented

Description:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Variables:

rhel_07_020720

Tags:

RHEL-07-020720 notimplemented

Notes:

Nothing to report

RHEL-07-020730 (V-72037)

The Red Hat Enterprise Linux operating system must be configured so that local initialization files do not execute world-writable programs.

Severity: Medium

Implementation Status: Not Implemented

Description:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Variables:

```
rhel_07_020730
```

Tags:

```
RHEL-07-020730  
notimplemented
```

Notes:

Nothing to report

RHEL-07-021010 (V-72043)

The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are used with removable media.

Severity: Medium

Implementation Status: Not Implemented

Description:

The “nosuid” mount option causes the system to not execute “setuid” and “setgid” files with owner privileges. This option must be used for mounting any file system not containing approved “setuid” and “setgid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Variables:

```
rhel_07_021010
```

Tags:

```
RHEL-07-021010  
notimplemented
```

Notes:

Nothing to report

RHEL-07-021040 (V-72049)

The Red Hat Enterprise Linux operating system must set the umask value to 077 for all local interactive user accounts.

Severity: Medium

Implementation Status: Not Implemented

Description:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be “0”. This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Variables:

rhel_07_021040

Tags:

RHEL-07-021040
notimplemented

Notes:

Nothing to report

RHEL-07-021600 (V-72069)

The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).

Severity: Low

Implementation Status: Not Implemented

Description:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Variables:

rhel_07_021600

Tags:

RHEL-07-021600
notimplemented

Notes:

Nothing to report

RHEL-07-021610 (V-72071)

The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify extended attributes.

Severity: Low

Implementation Status: Not Implemented

Description:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Variables:

rhel_07_021610

Tags:

RHEL-07-021610 notimplemented

Notes:

Nothing to report

RHEL-07-021700 (V-72075)

The Red Hat Enterprise Linux operating system must not allow removable media to be used as the boot loader unless approved.

Severity: Medium

Implementation Status: Not Implemented

Description:

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Variables:

rhel_07_021700

Tags:

RHEL-07-021700 notimplemented

Notes:

Nothing to report

RHEL-07-030201 (V-81017)

The Red Hat Enterprise Linux operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the “au-remote” plugin, the audisp-remote daemon will not off load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030210 (V-81019)

The Red Hat Enterprise Linux operating system must take appropriate action when the audisp-remote buffer is full.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When the remote buffer is full, audit logs will not be collected and sent to the central log server.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-030211 (V-81021)

The Red Hat Enterprise Linux operating system must label all off-loaded audit logs before sending them to the central log server.

Severity: Medium

Implementation Status: Not Implemented

Description:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-040100 (V-72219)

The Red Hat Enterprise Linux operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.

Severity: Medium

Implementation Status: Not Implemented

Description:

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Variables:

`rhel_07_040100`

Tags:

`RHEL-07-040100`
`notimplemented`

Notes:

Nothing to report

RHEL-07-040180 (V-72227)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

`rhel_07_040180`

Tags:

`RHEL-07-040180`
`ldap`
`notimplemented`

Notes:

Nothing to report

RHEL-07-040190 (V-72229)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

```
rhel_07_040190
```

Tags:

```
RHEL-07-040190  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040200 (V-72231)

The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

Severity: Medium

Implementation Status: Not Implemented

Description:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Variables:

```
rhel_07_040200
```

Tags:

```
RHEL-07-040200  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040510 (V-72271)

The Red Hat Enterprise Linux operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.

Severity: Medium

Implementation Status: Not Implemented

Description:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Variables:

--

Tags:

--

Notes:

Nothing to report

RHEL-07-040600 (V-72281)

For Red Hat Enterprise Linux operating systems using DNS resolution, at least two name servers must be configured.

Severity: Low

Implementation Status: Not Implemented

Description:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Variables:

rhel_07_040600

Tags:

RHEL-07-040600 notimplemented

Notes:

Nothing to report

RHEL-07-040750 (V-72311)

The Red Hat Enterprise Linux operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.

Severity: Medium

Implementation Status: Not Implemented

Description:

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Variables:

```
rhel_07_040750
```

Tags:

```
RHEL-07-040750  
notimplemented
```

Notes:

Nothing to report

RHEL-07-040810 (V-72315)

The Red Hat Enterprise Linux operating system access control program must be configured to grant or deny system access to specific hosts and services.

Severity: Medium

Implementation Status: Not Implemented

Description:

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Variables:

```
rhel_07_040810
```

Tags:

```
RHEL-07-040810  
notimplemented
```

Notes:

Nothing to report

2.4 Additional Controls

Although the Security Technical Implementation Guide (STIG) contains a very comprehensive set of security configurations, some contributors want to add extra security configurations to the role. The *contrib* portion of the role is designed to implement those configurations as an optional set of tasks.

In general, *contrib* controls are limited to items to meet backwards compatibility with the [Openstack Ansible Hardening](#) project. It is recommended that new *contrib* items (things that don't address specific STIG items) should be addressed in a separate Ansible role.

BELOW IS NOT YET IMPLEMENTED IN THIS ROLE

The below configurations and variables are not yet implemented. This page and message are being kept until it is implemented.

The *contrib* hardening configurations are disabled by default, but they can be enabled by setting the following Ansible variable:

```
rhel7stig_security_contrib_enabled: yes
```

The individual tasks are controlled by Ansible variables in `defaults/main.yml` that are defined under the `rhel7stig_security_contrib` variable.

2.4.1 Kernel

C-00001 - Disable IPv6

Some systems do not require IPv6 connectivity and the presence of link local IPv6 addresses can present an additional attack surface for lateral movement. Deployers can set the following variable to disable IPv6 on all network interfaces:

```
rhel7_stig_security_contrib:
  disable_ipv6: yes
```

Warning: Deployers should test this change in a test environment before applying it in a production deployment. Applying this change to a production system that relies on IPv6 connectivity will cause unexpected downtime.

2.5 Developer Guide

2.5.1 Building a development environment

NEED CONTENT

Insert dev environment setup and test running instructions.

2.5.2 Writing documentation

Documentation for individual controls is automatically generated where possible. There is also the ability to add deployer notes for individual tasks that discuss the specific implementation or risks with running the task/etc. Variables that control the execution of each task are automatically pulled from the Ansible task files themselves.

Deployer notes

Deployer notes are optional and can be added for each control that needs additional data to be provided to role users. The notes are simply rST (reStructuredText) fragments and can contain simple blocks of text or more complex rST formatted text. The system matches deployer notes to STIG controls based on the note filename, which should follow the format `RHEL-07-010010.rst`.

All of the notes are found within `doc/metadata/notes`. Here is an example:

```
The tasks in the security role enable the appropriate Linux Security Module
(LSM) for the operating system.

For Ubuntu, openSUSE and SUSE Linux Enterprise 12 systems, AppArmor is installed and
enabled. This change takes effect immediately.

For CentOS or Red Hat Enterprise Linux systems, SELinux is enabled (in
enforcing mode) and its user tools are automatically installed. If SELinux is
not in enforcing mode already, a reboot is required to enable SELinux and
relabel the filesystem.

.. warning::

    Relabeling a filesystem takes time and the server must be offline for the
    relabeling to complete. Filesystems with large amounts of files and
    filesystems on slow disks will cause the relabeling process to take more
    time.

Deployers can opt out of this change by setting the following Ansible variable:

.. code-block:: yaml

    rhel7stig_disruption_high: no
```

The note should be brief, but it must answer a few critical questions:

- What does the change do to a system?
- What is the value of making this change?
- How can a deployer opt out or opt in for a particular change?
- Is there additional documentation available online that may help a deployer decide whether or not this change is valuable to them?

Run `make html` from the `doc/` directory to rebuild the documentation and review your changes.

2.6 FAQ

2.6.1 Does this role work only with RHEL7?

No – it works on multiple distributions!

The RHEL7 STIG guidance is designed to ONLY be applicable to Red Hat Enterprise Linux 7 systems and if you are using this role in a regulated organization you should be aware that applying these settings to distributions other than RHEL or CentOS 7 is unsupported and may run afoul of your organization or regulatory bodies guidelines during a compliance audit. It is on YOU to understand your organizations requirements and the laws and regulations you must adhere to before applying this role.

See *Which systems are covered?* below for more details on applying this role to non-RedHat EL 7 or CentOS 7 systems.

2.6.2 Why should this role be applied to a system?

There are three main reasons to apply this role to production Linux systems:

Improve security posture The configurations from the STIG add security and rigor around multiple components of a Linux system, including user authentication, service configurations, and package management. All of these configurations add up to an environment that is more difficult for an attacker to penetrate and use for lateral movement.

Meet compliance requirements Some deployers may be subject to industry compliance programs, such as PCI-DSS, ISO 27001/27002, or NIST 800-53. Many of these programs require hardening standards to be applied to systems.

Deployment without disruption Security is often at odds with usability. The role provides the greatest security benefit without disrupting production systems. Deployers have the option to opt out or opt in for most configurations depending on how their environments are configured.

2.6.3 Which systems are covered?

This role and the STIG guidance it implements are fully applicable to servers (physical or virtual) and containers running the following Linux distributions:

- Red Hat Enterprise Linux 7
- CentOS 7

The plan is for this role to be functional for servers (physical or virtual) and containers running the following Linux distributions:

- Debian 8 Jessie **NOT YET FUNCTIONAL**
- Fedora 27 **NOT YET FUNCTIONAL**
- openSUSE Leap 42.2 and 42.3 **NOT YET FUNCTIONAL**
- SUSE Linux Enterprise 12 **NOT YET FUNCTIONAL**
- Ubuntu 16.04 Xenial (*deprecated see [Ansible Lockdown Ubuntu STIG](#)*)

The role is tested against each distribution to ensure that tasks run properly. For Red Hat Enterprise Linux 7 and CentOS 7 the role is tested to ensure it runs, it is idempotent, and OpenSCAP is used to run a compliance scan after the role is applied to test compliance with the STIG standard.

2.6.4 Which systems are not covered?

This role will run properly against a container (docker or other), however this is not recommended and is only really useful during the development and testing of this role (ie most CI systems provide containers and not full VMs), so this role must be able to run on and test against containers.

Again for those in the back... applying this role against a container in order to secure it is generally a *BAD* idea. You should be applying this role to your container hosts and then using other hardening guidance that is specific to the container technology you are using (docker, lxc, lxd, etc)

3.1 devel

- **Status:** Active development
- **STIG Version:** RHEL 7 Version 2, Release 1 (*Published on 2018-09-26*)
- **Supported Operating Systems:**
 - Red Hat Enterprise Linux 7
 - CentOS 7
- **Targeted Operating Systems:**

These are not yet supported but are on the target list.

- Debian 8 Jessie
- Fedora 26
- openSUSE Leap 42.2 and 42.3
- SUSE Linux Enterprise 12