RHEL 7 STIG Documentation

Release master

Major Hayden

Aug 11, 2017

Contents

Release: 1 Benchmark Date: 27 Feb 2017

CHAPTER 1

Cat I (High Severity)

High

V-71849 - The file permissions, ownership, and group membership of system files and commands must match the vendor values. - RHEL-07-010010

Severity

High

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

Fix

Run the following command to determine which package owns the file:

rpm -qf <filename>

Reset the permissions of files within a package with the following command:

#rpm –setperms <packagename>

Reset the user and group ownership of files within a package with the following command:

#rpm –setugids <packagename>

Check

Verify the file permissions, ownership, and group membership of system files and commands match the vendor values.

Check the file permissions, ownership, and group membership of system files and commands with the following command:

rpm -Va | grep '^.M'

If there is any output from the command indicating that the ownership or group of a system file or command, or a system file, has permissions less restrictive than the default, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001494, CCI-001496

V-71855 - The cryptographic hash of system files and commands must match vendor values. - RHEL-07-010020

Severity

High

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.

Fix

Run the following command to determine which package owns the file:

rpm -qf <filename>

The package can be reinstalled from a yum repository using the command:

sudo yum reinstall <packagename>

Alternatively, the package can be reinstalled from trusted media using the command:

sudo rpm -Uvh <packagename>

Check

Verify the cryptographic hash of system files and commands match the vendor values.

Check the cryptographic hash of system files and commands with the following command:

Note: System configuration files (indicated by a "c" in the second column) are expected to change over time. Unusual modifications should be investigated through the system audit log.

rpm -Va | grep '^..5'

If there is any output from the command for system binaries, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000663

V-71937 - The system must not have accounts configured with blank or null passwords. - RHEL-07-010290

Severity

High

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.

Fix

If an account is configured for password authentication but does not have an assigned password, it may be possible to log on to the account without authenticating.

Remove any instances of the "nullok" option in "/etc/pam.d/system-auth-ac" to prevent logons with empty passwords and run the "authconfig" command.

Check

To verify that null passwords cannot be used, run the following command:

grep nullok /etc/pam.d/system-auth-ac

If this produces any output, it may be possible to log on with accounts with empty passwords.

If null passwords can be used, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71939 - The SSH daemon must not allow authentication using an empty password. - RHEL-07-010300

Severity

High

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.

Fix

To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in "/etc/ssh/sshd_config":

PermitEmptyPasswords no

The SSH service must be restarted for changes to take effect. Any accounts with empty passwords should be disabled immediately, and PAM configuration should prevent users from being able to assign themselves empty passwords.

Check

To determine how the SSH daemon's "PermitEmptyPasswords" option is set, run the following command:

grep -i PermitEmptyPasswords /etc/ssh/sshd_config PermitEmptyPasswords no

If no line, a commented line, or a line indicating the value "no" is returned, the required value is set.

If the required value is not set, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000766

V-71953 - The operating system must not allow an unattended or automatic logon to the system via a graphical user interface. - RHEL-07-010440

Severity

High

Description

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

Fix

Configure the operating system to not allow an unattended or automatic logon to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Add or edit the line for the "AutomaticLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

[daemon] AutomaticLoginEnable=false

Check

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check for the value of the "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

grep -i automaticloginenable /etc/gdm/custom.conf AutomaticLoginEnable=false

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71955 - The operating system must not allow an unrestricted logon to the system. - RHEL-07-010450

Severity

High

Description

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

Fix

Configure the operating system to not allow an unrestricted account to log on to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Add or edit the line for the "TimedLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

[daemon] TimedLoginEnable=false

Check

Verify the operating system does not allow an unrestricted logon to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check for the value of the "TimedLoginEnable" parameter in "/etc/gdm/custom.conf" file with the following command:

grep -i timedloginenable /etc/gdm/custom.conf TimedLoginEnable=false

If the value of "TimedLoginEnable" is not set to "false", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71961 - Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. - RHEL-07-010480

Severity

High

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.

Fix

Configure the system to encrypt the boot password for root.

Generate an encrypted grub2 password for root with the following command:

Note: The hash generated is an example.

grub-mkpasswd-pbkdf2 Enter Password: Reenter Password: PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.F3A7CFAA5A51EED123BE8238C23B25B2A6909AFC9812F0D45

Using this hash, modify the "/etc/grub.d/10_linux" file with the following commands to add the password to the root entry:

cat << EOF > set superusers="root" password_pbkdf2 smithj grub.pbkdf2.sha512.10000.F3A7CFAA5A51EED123BE8238C23B25B2
> EOF

Generate a new "grub.conf" file with the new password with the following commands:

grub2-mkconfig –output=/tmp/grub2.cfg # mv /tmp/grub2.cfg /boot/grub2/grub.cfg

Check

Check to see if an encrypted root password is set. On systems that use a BIOS, use the following command:

grep -i password /boot/grub2/grub.cfg password_pbkdf2 superusers-account password-hash

If the root password entry does not begin with "password_pbkdf2", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000213

V-71963 - Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. - RHEL-07-010490

Severity

High

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.

Fix

Configure the system to encrypt the boot password for root.

Generate an encrypted grub2 password for root with the following command:

Note: The hash generated is an example.

grub-mkpasswd-pbkdf2 Enter Password: Reenter Password:

PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.F3A7CFAA5A51EED123BE8238C23B25B2A6909AFC9812F0D45

Using this hash, modify the "/etc/grub.d/10_linux" file with the following commands to add the password to the root entry:

cat << EOF > set superusers="root" password_pbkdf2 smithj grub.pbkdf2.sha512.10000.F3A7CFAA5A51EED123BE8238C23B25B2
> EOF

Generate a new "grub.conf" file with the new password with the following commands:

grub2-mkconfig –output=/tmp/grub2.cfg # mv /tmp/grub2.cfg /boot/efi/EFI/redhat/grub.cfg

Check

Check to see if an encrypted root password is set. On systems that use UEFI, use the following command:

grep -i password /boot/efi/EFI/redhat/grub.cfg password_pbkdf2 superusers-account password-hash

If the root password entry does not begin with "password_pbkdf2", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000213

V-71967 - The rsh-server package must not be installed. - RHEL-07-020000

Severity

High

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.

Fix

Configure the operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

yum remove rsh-server

Check

Check to see if the rsh-server package is installed with the following command:

yum list installed rsh-server

If the rsh-server package is installed, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000381

V-71969 - The ypserv package must not be installed. - RHEL-07-020010

Severity

High

Description

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

Fix

Configure the operating system to disable non-essential capabilities by removing the "ypserv" package from the system with the following command:

yum remove ypserv

Check

The NIS service provides an unencrypted authentication service that does not provide for the confidentiality and integrity of user passwords or the remote session.

Check to see if the "ypserve" package is installed with the following command:

yum list installed ypserv

If the "ypserv" package is installed, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000381

V-71977 - The 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. - RHEL-07-020050

Severity

High

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.

Fix

Configure the operating system to verify the signature of packages from a repository prior to install by setting the following option in the "/etc/yum.conf" file:

gpgcheck=1

Check

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components from a repository without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check that yum verifies the signature of packages from a repository prior to install with the following command:

grep gpgcheck /etc/yum.conf gpgcheck=1

If "gpgcheck" is not set to "1", or if options are missing or commented out, ask the System Administrator how the certificates for patches and other operating system components are verified.

If there is no process to validate certificates that is approved by the organization, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001749

V-71979 - The 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. - RHEL-07-020060

Severity

High

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.

Fix

Configure the operating system to verify the signature of local packages prior to install by setting the following option in the "/etc/yum.conf" file:

localpkg_gpgcheck=1

Check

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components of local packages without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check that yum verifies the signature of local packages prior to install with the following command:

grep localpkg_gpgcheck /etc/yum.conf localpkg_gpgcheck=1

If "localpkg_gpgcheck" is not set to "1", or if options are missing or commented out, ask the System Administrator how the signatures of local packages and other operating system components are verified.

If there is no process to validate the signatures of local packages that is approved by the organization, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-001749

V-71981 - The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of packages without verification of the repository metadata. - RHEL-07-020070

Severity

High

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 ensures 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 Certificate Authority.

Fix

Configure the operating system to verify the repository metadata by setting the following options in the "/etc/yum.conf" file:

repo_gpgcheck=1

Check

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components of local packages without verification of the repository metadata.

Check that yum verifies the package metadata prior to install with the following command:

grep repo_gpgcheck /etc/yum.conf repo_gpgcheck=1

If "repo_gpgcheck" is not set to "1", or if options are missing or commented out, ask the System Administrator how the metadata of local packages and other operating system components are verified.

If there is no process to validate the metadata of packages that is approved by the organization, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001749

V-71989 - The operating system must enable SELinux. - RHEL-07-020210

Severity

High

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.

Fix

Configure the operating system to verify correct operation of all security functions.

Set the “SELinux” status and the “Enforcing” mode by modifying the “/etc/selinux/config” file to have the following line:

SELINUX=enforcing

A reboot is required for the changes to take effect.

Check

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is active and in "Enforcing" mode with the following command:

getenforce Enforcing

If "SELinux" is not active and not in "Enforcing" mode, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002165, CCI-002696

V-71991 - The operating system must enable the SELinux targeted policy. - RHEL-07-020220

Severity

High

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.

Fix

Configure the operating system to verify correct operation of all security functions.

Set the "SELinuxtype" to the "targeted" policy by modifying the "/etc/selinux/config" file to have the following line:

SELINUXTYPE=targeted

A reboot is required for the changes to take effect.

Check

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is active and is enforcing the targeted policy with the following command:

sestatus SELinux status: enabled SELinuxfs mount: /selinu XCurrent mode: enforcing Mode from config file: enforcing Policy version: 24 Policy from config file: targeted

If the "Policy from config file" is not set to "targeted", or the "Loaded policy name" is not set to "targeted", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002165, CCI-002696

V-71993 - The x86 Ctrl-Alt-Delete key sequence must be disabled. - RHEL-07-020230

Severity

High

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.

Fix

Configure the system to disable the Ctrl-Alt_Delete sequence for the command line with the following command:

systemctl mask ctrl-alt-del.target

If GNOME is active on the system, create a database to contain the system-wide setting (if it does not already exist) with the following command:

cat /etc/dconf/db/local.d/00-disable-CAD

Add the setting to disable the Ctrl-Alt_Delete sequence for GNOME:

[org/gnome/settings-daemon/plugins/media-keys] logout=''

Check

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed.

Check that the ctrl-alt-del.service is not active with the following command:

systemctl status ctrl-alt-del.service reboot.target - Reboot

Loaded: loaded (/usr/lib/systemd/system/reboot.target; disabled) Active: inactive (dead)

Docs: man:systemd.special(7)

If the ctrl-alt-del.service is active, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71997 - The operating system must be a vendor supported release. - RHEL-07-020250

Severity

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.

Fix

Upgrade to a supported version of the operating system.

Check

Verify the version of the operating system is vendor supported.

Check the version of the operating system with the following command:

cat /etc/redhat-release

Red Hat Enterprise Linux Server release 7.2 (Maipo)

Current End of Life for RHEL 7.2 is Q4 2020.

Current End of Life for RHEL 7.3 is 30 June 2024.

If the release is not supported by the vendor, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72005 - The root account must be the only account having unrestricted access to the system. - RHEL-07-020310

Severity

High

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.

Fix

Change the UID of any account on the system, other than root, that has a UID of “0”.

If the account is associated with system commands or applications, the UID should be changed to one greater than “0” but less than “1000”. Otherwise, assign a UID of greater than “1000” that has not already been assigned.

Check

Check the system for duplicate UID “0” assignments with the following command:

awk -F: ‘$3 == 0 {print $1}’ /etc/passwd

If any accounts other than root have a UID of “0”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72067 - The 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. - RHEL-07-021350

Severity

High

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

Fix

Configure the operating system to implement DoD-approved encryption by installing the dracut-fips package.

To enable strict FIPS compliance, the fips=1 kernel option needs to be added to the kernel command line during system installation so key generation is done with FIPS-approved algorithms and continuous monitoring tests in place.

Configure the operating system to implement DoD-approved encryption by following the steps below:

The fips=1 kernel option needs to be added to the kernel command line during system installation so that key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users should also ensure that the system has plenty of entropy during the installation process by moving the mouse around, or if no mouse is available, ensuring that many keystrokes are typed. The recommended amount of keystrokes is 256 and more. Less than 256 keystrokes may generate a non-unique key.

For proper operation of the in-module integrity verification, the prelink has to be disabled. This can be done by configuring PRELINKING=no in the “/etc/sysconfig/prelink” configuration file. Existing prelinking, if any, should be undone on all system files using the prelink -u -a command.

Install the dracut-fips package with the following command:

yum install dracut-fips

Recreate the “initramfs” file with the following command:

Note: This command will overwrite the existing “initramfs” file.

dracut -f

Modify the kernel command line of the current kernel in the “grub.cfg” file by adding the following option to the GRUB_CMDLINE_LINUX key in the “/etc/default/grub” file and then rebuild the “grub.cfg” file:

fips=1

Changes to “/etc/default/grub” require rebuilding the “grub.cfg” file as follows:

On BIOS-based machines, use the following command:

grub2-mkconfig -o /boot/grub2/grub.cfg

On UEFI-based machines, use the following command:

grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg

If /boot or /boot/efi reside on separate partitions, the kernel parameter boot=<partition of /boot or /boot/efi> must be added to the kernel command line. You can identify a partition by running the df /boot or df /boot/efi command:

df /boot Filesystem 1K-blocks Used Available Use% Mounted on /dev/sda1 495844 53780 416464 12% /boot

To ensure the boot= configuration option will work even if device naming changes between boots, identify the universally unique identifier (UUID) of the partition with the following command:

blkid /dev/sda1 /dev/sda1: UUID=”05c000f1-a213-759e-c7a2-f11b7424c797” TYPE=”ext4”

For the example above, append the following string to the kernel command line:

boot=UUID=05c000f1-a213-759e-c7a2-f11b7424c797

Reboot the system for the changes to take effect.

Check

Verify the operating system implements DoD-approved encryption to protect the confidentiality of remote access sessions.

Check to see if the "dracut-fips" package is installed with the following command:

yum list installed | grep dracut-fips

dracut-fips-033-360.el7_2.x86_64.rpm

If a "dracut-fips" package is installed, check to see if the kernel command line is configured to use FIPS mode with the following command:

Note: GRUB 2 reads its configuration from the "/boot/grub2/grub.cfg" file on traditional BIOS-based machines and from the "/boot/efi/EFI/redhat/grub.cfg" file on UEFI machines.

grep fips /boot/grub2/grub.cfg /vmlinuz-3.8.0-0.40.el7.x86_64 root=/dev/mapper/rhel-root ro rd.md=0 rd.dm=0 rd.lvm.lv=rhel/swap crashkernel=auto rd.luks=0 vconsole.keymap=us rd.lvm.lv=rhel/root rhgb fips=1 quiet

If the kernel command line is configured to use FIPS mode, check to see if the system is in FIPS mode with the following command:

cat /proc/sys/crypto/fips_enabled 1

If a "dracut-fips" package is not installed, the kernel command line does not have a fips entry, or the system has a value of "0" for "fips_enabled" in "/proc/sys/crypto", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000068, CCI-001199, CCI-002450, CCI-002476

V-72077 - The telnet-server package must not be installed. - RHEL-07-021710

Severity

High

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.

Fix

Configure the operating system to disable non-essential capabilities by removing the telnet-server package from the system with the following command:

yum remove telnet-server

Check

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

The telnet service provides an unencrypted remote access service 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.

Check to see if the telnet-server package is installed with the following command:

yum list installed | grep telnet-server

If the telnet-server package is installed, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000381

V-72079 - Auditing must be 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. - RHEL-07-030000

Severity

High

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

Fix

Configure the operating system to produce audit records containing information to establish when (date and time) the events occurred.

Enable the auditd service with the following command:

chkconfig auditd on

Check

Verify the operating system produces audit records containing information to establish when (date and time) the events occurred.

Check to see if auditing is active by issuing the following command:

systemctl is-active auditd.service Active: active (running) since Tue 2015-01-27 19:41:23 EST; 22h ago

If the “auditd” status is not active, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000131

V-72213 - The system must use a DoD-approved virus scan program. - RHEL-07-032000

Severity

High

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.

Fix

Install an approved DoD antivirus solution on the system.

Check

Verify the system is using a DoD-approved virus scan program.

Check for the presence of "McAfee VirusScan Enterprise for Linux" with the following command:

systemctl status nails nails - service for McAfee VirusScan Enterprise for Linux > Loaded: loaded /opt/NAI/package/McAfeeVSEForLinux/McAfeeVSEForLinux-2.0.2.<build_number>; enabled) > Active: active (running) since Mon 2015-09-27 04:11:22 UTC;21 min ago

If the "nails" service is not active, check for the presence of "clamav" on the system with the following command:

 # systemctl status clamav-daemon.socket

systemctl status clamav-daemon.socket

clamav-daemon.socket - Socket for Clam AntiVirus userspace daemon Loaded: loaded (/lib/systemd/system/clamav-daemon.socket; enabled) Active: active (running) since Mon 2015-01-12 09:32:59 UTC; 7min ago

If neither of these applications are loaded and active, ask the System Administrator if there is an antivirus package installed and active on the system.

If no antivirus scan program is active on the system, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001668

V-72251 - The SSH daemon must be configured to only use the SSHv2 protocol. - RHEL-07-040390

Severity

High

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

Fix

Remove all Protocol lines that reference version "1" in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). The "Protocol" line must be as follows:

Protocol 2

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon is configured to only use the SSHv2 protocol.

Check that the SSH daemon is configured to only use the SSHv2 protocol with the following command:

grep -i protocol /etc/ssh/sshd_config Protocol 2 #Protocol 1,2

If any protocol line other than "Protocol 2" is uncommented, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000197, CCI-000366

V-72277 - There must be no .shosts files on the system. - RHEL-07-040540

Severity

High

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.

Fix

Remove any found ".shosts" files from the system.

rm /[path]/[to]/[file]/.shosts

Check

Verify there are no ".shosts" files on the system.

Check the system for the existence of these files with the following command:

find / -name '*.shosts'

If any ".shosts" files are found on the system, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72279 - There must be no shosts.equiv files on the system. - RHEL-07-040550

Severity

High

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.

Fix

Remove any found "shosts.equiv" files from the system.

rm /[path]/[to]/[file]/shosts.equiv

Check

Verify there are no “shosts.equiv” files on the system.

Check the system for the existence of these files with the following command:

find / -name shosts.equiv

If any “shosts.equiv” files are found on the system, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72299 - A File Transfer Protocol (FTP) server package must not be installed unless needed. - RHEL-07-040690

Severity

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.

Fix

Document the “lftpd” package with the ISSO as an operational requirement or remove it from the system with the following command:

yum remove lftpd

Check

Verify a lightweight FTP server has not been installed on the system.

Check to see if a lightweight FTP server has been installed with the following commands:

 # yum list installed lftpd lftp-4.4.8-7.el7.x86_64.rpm

If "lftpd" is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72301 - The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support. - RHEL-07-040700

Severity

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.

Fix

Remove the TFTP package from the system with the following command:

yum remove tftp

Check

Verify a TFTP server has not been installed on the system.

Check to see if a TFTP server has been installed with the following command:

yum list installed tftp-server tftp-server-0.49-9.el7.x86_64.rpm

If TFTP is installed and the requirement for TFTP is not documented with the ISSO, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72303 - Remote X connections for interactive users must be encrypted. - RHEL-07-040710

Severity

High

Description

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Fix

Configure SSH to encrypt connections for interactive users.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11Forwarding" keyword and set its value to "yes" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

X11Fowarding yes

The SSH service must be restarted for changes to take effect.

Check

Verify remote X connections for interactive users are encrypted.

Check that remote X connections are encrypted with the following command:

grep -i x11forwarding /etc/ssh/sshd_config X11Fowarding yes

If the "X11Forwarding" keyword is set to "no", is missing, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72313 - SNMP community strings must be changed from the default. - RHEL-07-040800

Severity

High

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.

Fix

If the "/etc/snmp/snmpd.conf" file exists, modify any lines that contain a community string value of "public" or "private" to another string value.

Check

Verify that a system using SNMP is not using default community strings.

Check to see if the "/etc/snmp/snmpd.conf" file exists with the following command:

 # ls -al /etc/snmp/snmpd.conf

-rw——- 1 root root 52640 Mar 12 11:08 snmpd.conf

If the file does not exist, this is Not Applicable.

If the file does exist, check for the default community strings with the following commands:

grep public /etc/snmp/snmpd.conf # grep private /etc/snmp/snmpd.conf

If either of these commands returns any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

CHAPTER 2

Cat II (Medium Severity)

Medium

V-71859 - The 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. - RHEL-07-010030

Severity

Medium

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."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read consent to terms in IS user agreem't."

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

Fix

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Create a database to contain the system-wide graphical user logon settings (if it does not already exist) with the following command:

touch /etc/dconf/db/local.d/01-banner-message

Add the following line to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

[org/gnome/login-screen] banner-message-enable=true

Check

Verify the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check to see if the operating system displays a banner at the logon screen with the following command:

grep banner-message-enable /etc/dconf/db/local.d/* banner-message-enable=true

If "banner-message-enable" is set to "false" or is missing, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000048

V-71861 - The 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. - RHEL-07-010040

Severity

Medium

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.”

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

“I’ve read consent to terms in IS user agreem’t.”

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

Fix

Configure the operating system to display the approved Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Create a database to contain the system-wide graphical user logon settings (if it does not already exist) with the following command:

touch /etc/dconf/db/local.d/01-banner-message

Add the following line to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

[org/gnome/login-screen] banner-message-text='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.'

Check

Verify the operating system displays the approved Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check that the operating system displays the exact approved Standard Mandatory DoD Notice and Consent Banner text with the command:

grep banner-message-text /etc/dconf/db/local.d/* banner-message-text= '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.'

If the banner does not match the approved Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000048

V-71863 - The 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. - RHEL-07-010050

Severity

Medium

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."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read consent to terms in IS user agreem't."

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

Fix

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via the command line by editing the "/etc/issue" file.

Replace the default text with the Standard Mandatory DoD Notice and Consent Banner. The DoD required text is:

"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."

Check

Verify the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon.

Check to see if the operating system displays a banner at the command line logon screen with the following command:

more /etc/issue

The command should return the following text: "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."

If the operating system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

If the text in the "/etc/issue" file does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000048

V-71891 - The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. - RHEL-07-010060

Severity

Medium

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

Fix

Configure the operating system to enable a user's session lock until that user re-establishes access using established identification and authentication procedures.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

touch /etc/dconf/db/local.d/00-screensaver

Edit "org/gnome/desktop/session" and add or update the following lines:

Set the lock time out to 900 seconds before the session is considered idle idle-delay=uint32 900

Edit "org/gnome/desktop/screensaver" and add or update the following lines:

Set this to true to lock the screen when the screensaver activates lock-enabled=true # Set the lock timeout to 180 seconds after the screensaver has been activated lock-delay=uint32 180

You must include the "uint32" along with the integer key values as shown.

Override the user's setting and prevent the user from changing it by editing "/etc/dconf/db/local.d/locks/screensaver" and adding or updating the following lines:

Lock desktop screensaver settings /org/gnome/desktop/session/idle-delay /org/gnome/desktop/screensaver/lock-enabled /org/gnome/desktop/screensaver/lock-delay

Update the system databases:

dconf update

Users must log out and back in again before the system-wide settings take effect.

Check

Verify the operating system enables a user's session lock until that user re-establishes access using established identification and authentication procedures. The screen program must be installed to lock sessions on the console.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check to see if the screen lock is enabled with the following command:

grep -i lock-enabled /etc/dconf/db/local.d/00-screensaver lock-enabled=true

If the "lock-enabled" setting is missing or is not set to "true", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000056

V-71893 - The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces. - RHEL-07-010070

Severity

Medium

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.

Fix

Configure the operating system to initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

touch /etc/dconf/db/local.d/00-screensaver

Edit "org/gnome/desktop/session" and add or update the following lines:

Set the lock time out to 900 seconds before the session is considered idle idle-delay=uint32 900

Edit "org/gnome/desktop/screensaver" and add or update the following lines:

Set this to true to lock the screen when the screensaver activates lock-enabled=true # Set the lock timeout to 180 seconds after the screensaver has been activated lock-delay=uint32 180

You must include the “uint32” along with the integer key values as shown.

Override the user’s setting and prevent the user from changing it by editing “/etc/dconf/db/local.d/locks/screensaver” and adding or updating the following lines:

Lock desktop screensaver settings /org/gnome/desktop/session/idle-delay /org/gnome/desktop/screensaver/lock-enabled /org/gnome/desktop/screensaver/lock-delay

Update the system databases:

dconf update

Users must log out and back in again before the system-wide settings take effect.

Check

Verify the operating system initiates a screensaver after a 15-minute period of inactivity for graphical user interfaces. The screen program must be installed to lock sessions on the console.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check to see if GNOME is configured to display a screensaver after a 15 minute delay with the following command:

grep -i idle-delay /etc/dconf/db/local.d/* idle-delay=uint32 900

If the “idle-delay” setting is missing or is not set to “900” or less, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-71895 - The operating system must set the idle delay setting for all connection types. - RHEL-07-010080

Severity

Medium

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.

Fix

Configure the operating system to prevent a user from overriding a session lock after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in /etc/dconf/profile/user, the file should be created under the appropriate subdirectory.

touch /etc/dconf/db/local.d/locks/session

Add the setting to lock the screensaver idle delay:

/org/gnome/desktop/screensaver/idle-delay

Check

Verify the operating system prevents a user from overriding session lock after a 15-minute period of inactivity for graphical user interfaces. The screen program must be installed to lock sessions on the console.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command: #grep system-db /etc/dconf/profile/user

system-db:local

Check for the lock delay setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

grep -i idle-delay /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/idle-delay

If the command does not return a result, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-71897 - The operating system must have the screen package installed. - RHEL-07-010090

Severity

Medium

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.

Fix

Install the screen package to allow the initiation a session lock after a 15-minute period of inactivity for graphical users interfaces.

Install the screen program (if it is not on the system) with the following command:

yum install screen

The console can now be locked with the following key combination:

ctrl+A x

Check

Verify the operating system has the screen package installed.

Check to see if the screen package is installed with the following command:

yum list installed | grep screen screen-4.3.1-3-x86_64.rpm

If is not installed, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-71899 - The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. - RHEL-07-010100

Severity

Medium

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.

Fix

Configure the operating system to initiate a session lock after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

touch /etc/dconf/db/local.d/00-screensaver

Add the setting to enable screensaver locking after 15 minutes of inactivity:

[org/gnome/desktop/screensaver]

idle-activation-enabled=true

Check

Verify the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces. The screen program must be installed to lock sessions on the console.

If it is installed, GNOME must be configured to enforce a session lock after a 15-minute delay. Check for the session lock settings with the following commands:

grep -i idle_activation_enabled /etc/dconf/db/local.d/* [org/gnome/desktop/screensaver] idle-activation-enabled=true

If “idle-activation-enabled” is not set to “true”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-71901 - The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. - RHEL-07-010110

Severity

Medium

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.

Fix

Configure the operating system to initiate a session lock for graphical user interfaces when a screensaver is activated.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

touch /etc/dconf/db/local.d/00-screensaver

Add the setting to enable session locking when a screensaver is activated:

[org/gnome/desktop/screensaver] lock-delay=uint32 5

After the setting has been set, run dconf update.

Check

Verify the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated. The screen program must be installed to lock sessions on the console.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

If GNOME is installed, check to see a session lock occurs when the screensaver is activated with the following command:

grep -i lock-delay /etc/dconf/db/local.d/* lock-delay=uint32 5

If the “lock-delay” setting is missing, or is not set, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-71903 - When passwords are changed or new passwords are established, the new password must contain at least one upper-case character. - RHEL-07-010120

Severity

Medium

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.

Fix

Configure the operating system to enforce password complexity by requiring that at least one upper-case character be used by setting the "ucredit" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

ucredit = -1

Check

Note: The value to require a number of upper-case characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "ucredit" in "/etc/security/pwquality.conf" with the following command:

grep ucredit /etc/security/pwquality.conf ucredit = -1

If the value of "ucredit" is not set to a negative value, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000192

V-71905 - When passwords are changed or new passwords are established, the new password must contain at least one lower-case character. - RHEL-07-010130

Severity

Medium

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.

Fix

Configure the operating system to lock an account for the maximum period when three unsuccessful logon attempts in 15 minutes are made.

Modify the first three lines of the "auth" section of the "/etc/pam.d/system-auth-ac" and "/etc/pam.d/password-auth-ac" files to match the following lines:

Note: RHEL 7.3 and later allows for a value of "never" for "unlock_time". This is an acceptable value but should be used with caution if availability is a concern.

auth required pam_faillock.so preauth silent audit deny=3 even_deny_root fail_interval=900 unlock_time=604800 auth sufficient pam_unix.so try_first_pass auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root fail_interval=900 unlock_time=604800

and run the "authconfig" command.

Check

Note: The value to require a number of lower-case characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "lcredit" in "/etc/security/pwquality.conf" with the following command:

grep lcredit /etc/security/pwquality.conf lcredit = -1

If the value of "lcredit" is not set to a negative value, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000193

V-71907 - When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character. - RHEL-07-010140

Severity

Medium

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.

Fix

Configure the operating system to enforce password complexity by requiring that at least one numeric character be used by setting the “dcredit” option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

dcredit = -1

Check

Note: The value to require a number of numeric characters to be set is expressed as a negative number in “/etc/security/pwquality.conf”.

Check the value for “dcredit” in “/etc/security/pwquality.conf” with the following command:

grep dcredit /etc/security/pwquality.conf dcredit = -1

If the value of “dcredit” is not set to a negative value, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000194

V-71909 - When passwords are changed or new passwords are assigned, the new password must contain at least one special character. - RHEL-07-010150

Severity

Medium

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.

Fix

Configure the operating system to enforce password complexity by requiring that at least one special character be used by setting the “dcredit” option.

Add the following line to “/etc/security/pwquality.conf” (or modify the line to have the required value):

ocredit = -1

Check

Verify the operating system enforces password complexity by requiring that at least one special character be used.

Note: The value to require a number of special characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "ocredit" in "/etc/security/pwquality.conf" with the following command:

grep ocredit /etc/security/pwquality.conf ocredit=-1

If the value of "ocredit" is not set to a negative value, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001619

V-71911 - When passwords are changed a minimum of eight of the total number of characters must be changed. - RHEL-07-010160

Severity

Medium

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.

Fix

Configure the operating system to require the change of at least eight of the total number of characters when passwords are changed by setting the “difok” option.

Add the following line to “/etc/security/pwquality.conf” (or modify the line to have the required value):

difok = 8

Check

The “difok” option sets the number of characters in a password that must not be present in the old password.

Check for the value of the “difok” option in “/etc/security/pwquality.conf” with the following command:

grep difok /etc/security/pwquality.conf difok = 8

If the value of “difok” is set to less than “8”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000195

V-71913 - When passwords are changed a minimum of four character classes must be changed. - RHEL-07-010170

Severity

Medium

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.

Fix

Configure the operating system to require the change of at least four character classes when passwords are changed by setting the "minclass" option.

Add the following line to "/etc/security/pwquality.conf conf" (or modify the line to have the required value):

minclass = 4

Check

The "minclass" option sets the minimum number of required classes of characters for the new password (digits, uppercase, lower-case, others).

Check for the value of the "minclass" option in "/etc/security/pwquality.conf" with the following command:

grep minclass /etc/security/pwquality.conf minclass = 4

If the value of "minclass" is set to less than "4", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000195

V-71915 - When passwords are changed the number of repeating consecutive characters must not be more than four characters. - RHEL-07-010180

Severity

Medium

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.

Fix

Configure the operating system to require the change of the number of repeating consecutive characters when passwords are changed by setting the "maxrepeat" option.

Add the following line to "/etc/security/pwquality.conf conf" (or modify the line to have the required value):

maxrepeat = 2

Check

The "maxrepeat" option sets the maximum number of allowed same consecutive characters in a new password.

Check for the value of the "maxrepeat" option in "/etc/security/pwquality.conf" with the following command:

grep maxrepeat /etc/security/pwquality.conf maxrepeat = 2

If the value of "maxrepeat" is set to more than "2", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000195

V-71917 - When passwords are changed the number of repeating characters of the same character class must not be more than four characters. - RHEL-07-010190

Severity

Medium

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.

Fix

Configure the operating system to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option.

Add the following line to "/etc/security/pwquality.conf" conf (or modify the line to have the required value):

maxclassrepeat = 4

Check

The "maxclassrepeat" option sets the maximum number of allowed same consecutive characters in the same class in the new password.

Check for the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" with the following command:

grep maxclassrepeat /etc/security/pwquality.conf maxclassrepeat = 4

If the value of "maxclassrepeat" is set to more than "4", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000195

V-71919 - The PAM system service must be configured to store only encrypted representations of passwords. - RHEL-07-010200

Severity

Medium

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.

Fix

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add the following line in "/etc/pam.d/system-auth-ac":

password sufficient pam_unix.so sha512

and run the "authconfig" command.

Check

Verify the PAM system service is configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is SHA512.

Check that the system is configured to create SHA512 hashed passwords with the following command:

grep password /etc/pam.d/system-auth-ac password sufficient pam_unix.so sha512

If the "/etc/pam.d/system-auth-ac" configuration files allow for password hashes other than SHA512 to be used, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000196

V-71921 - The shadow file must be configured to store only encrypted representations of passwords. - RHEL-07-010210

Severity

Medium

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.

Fix

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add or update the following line in "/etc/login.defs":

ENCRYPT_METHOD SHA512

Check

Verify the system's shadow file is configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is SHA512.

Check that the system is configured to create SHA512 hashed passwords with the following command:

grep -i encrypt /etc/login.defs ENCRYPT_METHOD SHA512

If the "/etc/login.defs" configuration file does not exist or allows for password hashes other than SHA512 to be used, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000196

V-71923 - User and group account administration utilities must be configured to store only encrypted representations of passwords. - RHEL-07-010220

Severity

Medium

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.

Fix

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add or update the following line in "/etc/libuser.conf" in the [defaults] section:

crypt_style = sha512

Check

Verify the user and group account administration utilities are configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is "SHA512".

Check that the system is configured to create "SHA512" hashed passwords with the following command:

cat /etc/libuser.conf | grep -i sha512

crypt_style = sha512

If the "crypt_style" variable is not set to "sha512", is not in the defaults section, or does not exist, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None

- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000196

V-71925 - Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime. - RHEL-07-010230

Severity

Medium

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.

Fix

Configure the operating system to enforce 24 hours/1 day as the minimum password lifetime.

Add the following line in "/etc/login.defs" (or modify the line to have the required value):

PASS_MIN_DAYS 1

Check

Verify the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts.

Check for the value of "PASS_MIN_DAYS" in "/etc/login.defs" with the following command:

grep -i pass_min_days /etc/login.defs PASS_MIN_DAYS 1

If the "PASS_MIN_DAYS" parameter value is not "1" or greater, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None

- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000198

V-71927 - Passwords must be restricted to a 24 hours/1 day minimum lifetime. - RHEL-07-010240

Severity

Medium

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.

Fix

Configure non-compliant accounts to enforce a 24 hours/1 day minimum password lifetime:

chage -m 1 [user]

Check

Check whether the minimum time period between password changes for each user account is one day or greater.

awk -F: '$4 < 1 {print $1}' /etc/shadow

If any results are returned that are not associated with a system account, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000198

V-71929 - Passwords for new users must be restricted to a 60-day maximum lifetime. - RHEL-07-010250

Severity

Medium

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.

Fix

Configure the operating system to enforce a 60-day maximum password lifetime restriction.

Add the following line in "/etc/login.defs" (or modify the line to have the required value):

PASS_MAX_DAYS 60

Check

Verify the operating system enforces a 60-day maximum password lifetime restriction for new user accounts.

Check for the value of "PASS_MAX_DAYS" in "/etc/login.defs" with the following command:

grep -i pass_max_days /etc/login.defs PASS_MAX_DAYS 60

If the "PASS_MAX_DAYS" parameter value is not 60 or less, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None

- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000199

V-71931 - Existing passwords must be restricted to a 60-day maximum lifetime. - RHEL-07-010260

Severity

Medium

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.

Fix

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.

chage -M 60 [user]

Check

Check whether the maximum time period for existing passwords is restricted to 60 days.

awk -F: '$5 > 60 {print $1}' /etc/shadow

If any results are returned that are not associated with a system account, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000199

V-71933 - Passwords must be prohibited from reuse for a minimum of five generations. - RHEL-07-010270

Severity

Medium

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.

Fix

Configure the operating system to prohibit password reuse for a minimum of five generations.

Add the following line in "/etc/pam.d/system-auth-ac" (or modify the line to have the required value):

password sufficient pam_unix.so use_authtok sha512 shadow remember=5

and run the "authconfig" command.

Check

Verify the operating system prohibits password reuse for a minimum of five generations.

Check for the value of the "remember" argument in "/etc/pam.d/system-auth-ac" with the following command:

grep -i remember /etc/pam.d/system-auth-ac password sufficient pam_unix.so use_authtok sha512 shadow remember=5

If the line containing the "pam_unix.so" line does not have the "remember" module argument set, or the value of the "remember" module argument is set to less than "5", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000200

V-71935 - Passwords must be a minimum of 15 characters in length. - RHEL-07-010280

Severity

Medium

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.

Fix

Configure operating system to enforce a minimum 15-character password length.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

minlen = 15

Check

Verify the operating system enforces a minimum 15-character password length. The "minlen" option sets the minimum number of characters in a new password.

Check for the value of the "minlen" option in "/etc/security/pwquality.conf" with the following command:

grep minlen /etc/security/pwquality.conf minlen = 15

If the command does not return a "minlen" value of 15 or greater, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000205

V-71941 - The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. - RHEL-07-010310

Severity

Medium

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.

Fix

Configure the operating system to disable account identifiers (individuals, groups, roles, and devices) after the password expires.

Add the following line to "/etc/default/useradd" (or modify the line to have the required value):

INACTIVE=0

Check

Verify the operating system disables account identifiers (individuals, groups, roles, and devices) after the password expires with the following command:

grep -i inactive /etc/default/useradd INACTIVE=0

If the value is not set to "0", is commented out, or is not defined, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000795

V-71943 - Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period. - RHEL-07-010320

Severity

Medium

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

Fix

Configure the operating system to lock an account for the maximum period when three unsuccessful logon attempts in 15 minutes are made.

Modify the first three lines of the auth section of the "/etc/pam.d/system-auth-ac" and "/etc/pam.d/password-auth-ac" files to match the following lines:

auth required pam_faillock.so preauth silent audit deny=3 even_deny_root fail_interval=900 unlock_time=604800 auth sufficient pam_unix.so try_first_pass auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root fail_interval=900 unlock_time=604800

and run the "authconfig" command.

Check

Verify the operating system automatically locks an account for the maximum period for which the system can be configured.

Check that the system locks an account for the maximum period after three unsuccessful logon attempts within a period of 15 minutes with the following command:

grep pam_faillock.so /etc/pam.d/password-auth-ac auth required pam_faillock.so preauth silent audit deny=3 even_deny_root unlock_time=604800 auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root unlock_time=604800

If the "unlock_time" setting is greater than "604800" on both lines with the "pam_faillock.so" module name or is missing from a line, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002238

V-71945 - If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. - RHEL-07-010330

Severity

Medium

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

Fix

Configure the operating system to automatically lock the root account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes are made.

Modify the first three lines of the auth section of the “/etc/pam.d/system-auth-ac” and “/etc/pam.d/password-auth-ac” files to match the following lines:

auth required pam_faillock.so preauth silent audit deny=3 even_deny_root fail_interval=900 unlock_time=604800 auth sufficient pam_unix.so try_first_pass auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root fail_interval=900 unlock_time=604800

and run the “authconfig” command.

Check

Verify the operating system automatically locks the root account until it is released by an administrator when three unsuccessful logon attempts in 15 minutes are made.

grep pam_faillock.so /etc/pam.d/password-auth-ac auth required pam_faillock.so preauth silent audit deny=3 even_deny_root fail_interval=900 auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root fail_interval=900

If the "even_deny_root" setting is not defined on both lines with the "pam_faillock.so" module name, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002238

V-71947 - Users must provide a password for privilege escalation. - RHEL-07-010340

Severity

Medium

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

Fix

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

grep -i nopasswd /etc/sudoers /etc/sudoers.d/*

Remove any occurrences of "NOPASSWD" tags in the file.

Check

Verify the operating system requires users to supply a password for privilege escalation.

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

grep -i nopasswd /etc/sudoers /etc/sudoers.d/*

If any uncommented line is found with a "NOPASSWD" tag, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002038

V-71949 - Users must re-authenticate for privilege escalation. - RHEL-07-010350

Severity

Medium

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

Fix

Configure the operating system to require users to reauthenticate for privilege escalation.

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

Remove any occurrences of "!authenticate" tags in the file.

Check

Verify the operating system requires users to reauthenticate for privilege escalation.

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

grep -i authenticate /etc/sudoers /etc/sudoers.d/*

If any line is found with a "!authenticate" tag, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002038

V-71951 - The delay between logon prompts following a failed console logon attempt must be at least four seconds. - RHEL-07-010430

Severity

Medium

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.

Fix

Configure the operating system to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.

Modify the "/etc/login.defs" file to set the "FAIL_DELAY" parameter to "4" or greater:

FAIL_DELAY 4

Check

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt.

Check the value of the "fail_delay" parameter in the "/etc/login.defs" file with the following command:

grep -i fail_delay /etc/login.defs FAIL_DELAY 4

If the value of "FAIL_DELAY" is not set to "4" or greater, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71957 - The operating system must not allow users to override SSH environment variables. - RHEL-07-010460

Severity

Medium

Description

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

Fix

Configure the operating system to not allow users to override environment variables to the SSH daemon.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for "PermitUserEnvironment" keyword and set the value to "no":

PermitUserEnvironment no

The SSH service must be restarted for changes to take effect.

Check

Verify the operating system does not allow users to override environment variables to the SSH daemon.

Check for the value of the "PermitUserEnvironment" keyword with the following command:

grep -i permituserenvironment /etc/ssh/sshd_config PermitUserEnvironment no

If the "PermitUserEnvironment" keyword is not set to "no", is missing, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71959 - The operating system must not allow a non-certificate trusted host SSH logon to the system. - RHEL-07-010470

Severity

Medium

Description

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

Fix

Configure the operating system to not allow a non-certificate trusted host SSH logon to the system.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for "HostbasedAuthentication" keyword and set the value to "no":

HostbasedAuthentication no

The SSH service must be restarted for changes to take effect.

Check

Verify the operating system does not allow a non-certificate trusted host SSH logon to the system.

Check for the value of the "HostbasedAuthentication" keyword with the following command:

grep -i hostbasedauthentication /etc/ssh/sshd_config HostbasedAuthentication no

If the "HostbasedAuthentication" keyword is not set to "no", is missing, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71965 - The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication. - RHEL-07-010500

Severity

Medium

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

Fix

Configure the operating system to require individuals to be authenticated with a multifactor authenticator.

Enable smartcard logons with the following commands:

authconfig –enablesmartcard –smartcardaction=1 –update # authconfig –enablerequiresmartcard -update

Modify the "/etc/pam_pkcs11/pkcs11_eventmgr.conf" file to uncomment the following line:

#/usr/X11R6/bin/xscreensaver-command -lock

Modify the "/etc/pam_pkcs11/pam_pkcs11.conf" file to use the cackey module if required.

Check

Verify the operating system requires multifactor authentication to uniquely identify organizational users using multifactor authentication.

Check to see if smartcard authentication is enforced on the system:

authconfig –test | grep -i smartcard

The entry for use only smartcard for logon may be enabled, and the smartcard module and smartcard removal actions must not be blank.

If smartcard authentication is disabled or the smartcard and smartcard removal actions are blank, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000766

V-71971 - The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. - RHEL-07-020020

Severity

Medium

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.

Fix

Configure the operating system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Use the following command to map a new user to the “sysdam_u” role:

#semanage login -a -s sysadm_u <username>

Use the following command to map an existing user to the “sysdam_u” role:

#semanage login -m -s sysadm_u <username>

Use the following command to map a new user to the “staff_u” role:

#semanage login -a -s staff_u <username>

Use the following command to map an existing user to the “staff_u” role:

#semanage login -m -s staff_u <username>

Use the following command to map a new user to the “user_u” role:

semanage login -a -s user_u <username>

Use the following command to map an existing user to the “user_u” role:

semanage login -m -s user_u <username>

Check

Verify the operating system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Get a list of authorized users (other than System Administrator and guest accounts) for the system.

Check the list against the system by using the following command:

semanage login -l | more Login Name SELinux User MLS/MCS Range Service __default__ user_u s0-s0:c0.c1023 * root unconfined_u s0-s0:c0.c1023 * system_u system_u s0-s0:c0.c1023 * joe staff_u s0-s0:c0.c1023 *

All administrators must be mapped to the "sysadm_u" or "staff_u" users with the appropriate domains (sysadm_t and staff_t).

All authorized non-administrative users must be mapped to the "user_u" role or the appropriate domain (user_t).

If they are not mapped in this way, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002165, CCI-002235

V-71973 - A file integrity tool must verify the baseline operating system configuration at least weekly. - RHEL-07-020030

Severity

Medium

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.

Fix

Configure the file integrity tool to automatically run on the system at least weekly. The following example output is generic. It will set cron to run AIDE daily, but other file integrity tools may be used:

cat /etc/cron.daily/aide 0 0 * * * /usr/sbin/aide –check | /bin/mail -s “aide integrity check run for <system name>” root@sysname.mil

Check

Verify the operating system routinely checks the baseline configuration for unauthorized changes.

Note: A file integrity tool other than Advanced Intrusion Detection Environment (AIDE) may be used, but the tool must be executed at least once per week.

Check to see if AIDE is installed on the system with the following command:

yum list installed aide

If AIDE is not installed, ask the SA how file integrity checks are performed on the system.

Check for the presence of a cron job running daily or weekly on the system that executes AIDE daily to scan for changes to the system baseline. The command used in the example will use a daily occurrence.

Check the “/etc/cron.daily” subdirectory for a “crontab” file controlling the execution of the file integrity application. For example, if AIDE is installed on the system, use the following command:

ls -al /etc/cron.* | grep aide -rwxr-xr-x 1 root root 29 Nov 22 2015 aide

If the file integrity application does not exist, or a “crontab” file does not exist in the “/etc/cron.daily” or “/etc/cron.weekly” subdirectories, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001744

V-71975 - Designated personnel must be notified if baseline configurations are changed in an unauthorized manner. - RHEL-07-020040

Severity

Medium

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.

Fix

Configure the operating system to notify designated personnel if baseline configurations are changed in an unauthorized manner. The AIDE tool can be configured to email designated personnel through the use of the cron system.

The following example output is generic. It will set cron to run AIDE daily and to send email at the completion of the analysis.

more /etc/cron.daily/aide 0 0 * * * /usr/sbin/aide –check | /bin/mail -s "$HOSTNAME - Daily aide integrity check run" root@sysname.mil

Check

Verify the operating system notifies designated personnel if baseline configurations are changed in an unauthorized manner.

Note: A file integrity tool other than Advanced Intrusion Detection Environment (AIDE) may be used, but the tool must be executed and notify specified individuals via email or an alert.

Check to see if AIDE is installed on the system with the following command:

yum list installed aide

If AIDE is not installed, ask the SA how file integrity checks are performed on the system.

Check for the presence of a cron job running routinely on the system that executes AIDE to scan for changes to the system baseline. The commands used in the example will use a daily occurrence.

Check the "/etc/cron.daily" subdirectory for a "crontab" file controlling the execution of the file integrity application. For example, if AIDE is installed on the system, use the following commands:

ls -al /etc/cron.daily | grep aide -rwxr-xr-x 1 root root 32 Jul 1 2011 aide

AIDE does not have a configuration that will send a notification, so the cron job uses the mail application on the system to email the results of the file integrity run as in the following example:

more /etc/cron.daily/aide 0 0 * * * /usr/sbin/aide –check | /bin/mail -s "$HOSTNAME - Daily aide integrity check run" root@sysname.mil

If the file integrity application does not notify designated personnel of changes, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001744

V-71983 - USB mass storage must be disabled. - RHEL-07-020100

Severity

Medium

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

Fix

Configure the operating system to disable the ability to use USB mass storage devices.

Create a file under "/etc/modprobe.d" with the following command:

#touch /etc/modprobe.d/nousbstorage

Add the following line to the created file:

install usb-storage /bin/true

Check

If there is an HBSS with a Device Control Module and a Data Loss Prevention mechanism, this requirement is not applicable.

Verify the operating system disables the ability to use USB mass storage devices.

Check to see if USB mass storage is disabled with the following command:

#grep -i usb-storage /etc/modprobe.d/*

install usb-storage /bin/true

If the command does not return any output, and use of USB storage devices is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366, CCI-000778, CCI-001958

V-71985 - File system automounter must be disabled unless required. - RHEL-07-020110

Severity

Medium

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

Fix

Configure the operating system to disable the ability to automount devices.

Turn off the automount service with the following command:

systemctl disable autofs

If “autofs” is required for Network File System (NFS), it must be documented with the ISSO.

Check

Verify the operating system disables the ability to automount devices.

Check to see if automounter service is active with the following command:

systemctl status autofs autofs.service - Automounts filesystems on demand

Loaded: loaded (/usr/lib/systemd/system/autofs.service; disabled) Active: inactive (dead)

If the "autofs" status is set to "active" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366, CCI-000778, CCI-001958

V-71995 - The 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. - RHEL-07-020240

Severity

Medium

Description

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

Fix

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the line for the "UMASK" parameter in "/etc/login.defs" file to "077":

UMASK 077

Check

Verify the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Check for the value of the "UMASK" parameter in "/etc/login.defs" file with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in "/etc/login.defs" file, the Severity is raised to a CAT I.

grep -i umask /etc/login.defs UMASK 077

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-71999 - Vendor packaged system security patches and updates must be installed and up to date. - RHEL-07-020260

Severity

Medium

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.

Fix

Install the operating system patches or updated packages available from Red Hat within 30 days or sooner as local policy dictates.

Check

Verify the operating system security patches and updates are installed and up to date. Updates are required to be applied with a frequency determined by the site or Program Management Office (PMO).

Obtain the list of available package security updates from Red Hat. The URL for updates is https://rhn.redhat.com/errata/. It is important to note that updates provided by Red Hat may not be present on the system if the underlying packages are not installed.

Check that the available package security updates have been installed on the system with the following command:

yum history list | more Loaded plugins: langpacks, product-id, subscription-manager ID | Command line | Date and time | Action(s) | Altered ——————————————————————————-

> 70 | install aide | 2016-05-05 10:58 | Install | 1 69 | update -y | 2016-05-04 14:34 | Update | 18 EE 68 | install vlc | 2016-04-21 17:12 | Install | 21 67 | update -y | 2016-04-21 17:04 | Update | 7 EE 66 | update -y | 2016-04-15 16:47 | E, I, U | 84 EE

If package updates have not been performed on the system within the timeframe that the site/program documentation requires, this is a finding.

Typical update frequency may be overridden by Information Assurance Vulnerability Alert (IAVA) notifications from CYBERCOM.

If the operating system is in non-compliance with the Information Assurance Vulnerability Management (IAVM) process, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None

- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72001 - The system must not have unnecessary accounts. - RHEL-07-020270

Severity

Medium

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.

Fix

Configure the system so all accounts on the system are assigned to an active system, application, or user account.

Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.

Document all authorized accounts on the system.

Check

Verify all accounts on the system are assigned to an active system, application, or user account.

Obtain the list of authorized system accounts from the Information System Security Officer (ISSO).

Check the system accounts on the system with the following command:

more /etc/passwd root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

Accounts such as “games” and “gopher” are not authorized accounts as they do not support authorized system functions.

If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72007 - All files and directories must have a valid owner. - RHEL-07-020320

Severity

Medium

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.

Fix

Either remove all files and directories from the system that do not have a valid user, or assign a valid user to all unowned files and directories on the system with the “chown” command:

chown <user> <file>

Check

Verify all files and directories on the system have a valid owner.

Check the owner of all files and directories with the following command:

Note: The value after -fstype must be replaced with the filesystem type. XFS is used as an example.

find / -xdev -fstype xfs -nouser

If any files on the system do not have an assigned owner, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None

- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002165

V-72009 - All files and directories must have a valid group owner. - RHEL-07-020330

Severity

Medium

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.

Fix

Either remove all files and directories from the system that do not have a valid group, or assign a valid group to all files and directories on the system with the "chgrp" command:

chgrp <group> <file>

Check

Verify all files and directories on the system have a valid group.

Check the owner of all files and directories with the following command:

Note: The value after -fstype must be replaced with the filesystem type. XFS is used as an example.

find / -xdev -fstype xfs -nogroup

If any files on the system do not have an assigned group, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None

- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002165

V-72011 - All local interactive users must have a home directory assigned in the /etc/passwd file. - RHEL-07-020600

Severity

Medium

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.

Fix

Assign home directories to all local interactive users that currently do not have a home directory assigned.

Check

Verify local interactive users on the system have a home directory assigned.

Check for missing local interactive user home directories with the following command:

pwck -r user ‘lp’: directory ‘/var/spool/lpd’ does not exist user ‘news’: directory ‘/var/spool/news’ does not exist user ‘uucp’: directory ‘/var/spool/uucp’ does not exist user ‘smithj’: directory ‘/home/smithj’ does not exist

Ask the System Administrator (SA) if any users found without home directories are local interactive users. If the SA is unable to provide a response, check for users with a User Identifier (UID) of 1000 or greater with the following command:

cut -d: -f 1,3 /etc/passwd | egrep ”:[1-4][0-9]{2}$|:[0-9]{1,2}$”

If any interactive users do not have a home directory assigned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72013 - All local interactive user accounts, upon creation, must be assigned a home directory. - RHEL-07-020610

Severity

Medium

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.

Fix

Configure the operating system to assign home directories to all new local interactive users by setting the "CREATE_HOME" parameter in "/etc/login.defs" to "yes" as follows.

CREATE_HOME yes

Check

Verify all local interactive users on the system are assigned a home directory upon creation.

Check to see if the system is configured to create home directories for local interactive users with the following command:

grep -i create_home /etc/login.defs CREATE_HOME yes

If the value for "CREATE_HOME" parameter is not set to "yes", the line is missing, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72015 - All local interactive user home directories defined in the /etc/passwd file must exist. - RHEL-07-020620

Severity

Medium

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.

Fix

Create home directories to all local interactive users that currently do not have a home directory assigned. Use the following commands to create the user home directory assigned in "/etc/ passwd":

Note: The example will be for the user smithj, who has a home directory of "/home/smithj", a UID of "smithj", and a Group Identifier (GID) of "users assigned" in "/etc/passwd".

mkdir /home/smithj # chown smithj /home/smithj # chgrp users /home/smithj # chmod 0750 /home/smithj

Check

Verify the assigned home directory of all local interactive users on the system exists.

Check the home directory assignment for all local interactive non-privileged users on the system with the following command:

cut -d: -f 1,3 /etc/passwd | egrep ":[1-9][0-9]{2}$|:[0-9]{1,2}$" smithj /home/smithj

Note: This may miss interactive users that have been assigned a privileged UID. Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check that all referenced home directories exist with the following command:

pwck -r user 'smithj': directory '/home/smithj' does not exist

If any home directories referenced in "/etc/passwd" are returned as not defined, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72017 - All local interactive user home directories must have mode 0750 or less permissive. - RHEL-07-020630

Severity

Medium

Description

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

Fix

Change the mode of interactive user's home directories to "0750". To change the mode of a local interactive user's home directory, use the following command:

Note: The example will be for the user "smithj".

chmod 0750 /home/smithj

Check

Verify the assigned home directory of all local interactive users has a mode of "0750" or less permissive.

Check the home directory assignment for all non-privileged users on the system with the following command:

Note: This may miss interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.

ls -ld $ (egrep ':[0-9]{4}' /etc/passwd | cut -d: -f6) -rwxr-x— 1 smithj users 18 Mar 5 17:06 /home/smithj

If home directories referenced in "/etc/passwd" do not have a mode of "0750" or less permissive, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72019 - All local interactive user home directories must be owned by their respective users. - RHEL-07-020640

Severity

Medium

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.

Fix

Change the owner of a local interactive user's home directories to that owner. To change the owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj".

chown smithj /home/smithj

Check

Verify the assigned home directory of all local interactive users on the system exists.

Check the home directory assignment for all local interactive non-privileged users on the system with the following command:

Note: This may miss interactive users that have been assigned a privileged UID. Evidence of interactive use may be obtained from a number of log files containing system logon information.

ls -ld $ (egrep ':[0-9]{4}' /etc/passwd | cut -d: -f6) -rwxr-x— 1 smithj users 18 Mar 5 17:06 /home/smithj

If any home directories referenced in "/etc/passwd" are returned as not defined, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72021 - All local interactive user home directories must be group-owned by the home directory owners primary group. - RHEL-07-020650

Severity

Medium

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.

Fix

Change the group owner of a local interactive user's home directory to the group found in "/etc/passwd". To change the group owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj", and has a primary group of users.

chgrp users /home/smithj

Check

Verify the assigned home directory of all local interactive users is group-owned by that user's primary GID.

Check the home directory assignment for all non-privileged users on the system with the following command:

Note: This may miss local interactive users that have been assigned a privileged UID. Evidence of interactive use may be obtained from a number of log files containing system logon information.

ls -ld $ (egrep ':[0-9]{4}' /etc/passwd | cut -d: -f6) -rwxr-x— 1 smithj users 18 Mar 5 17:06 /home/smithj

Check the user's primary group with the following command:

grep users /etc/group users:x:250:smithj,jonesj,jacksons

If the user home directory referenced in "/etc/passwd" is not group-owned by that user's primary GID, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72023 - All files and directories contained in local interactive user home directories must be owned by the owner of the home directory. - RHEL-07-020660

Severity

Medium

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.

Fix

Change the owner of a local interactive user's files and directories to that owner. To change the owner of a local interactive user's files and directories, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj".

chown smithj /home/smithj/<file or directory>

Check

Verify all files and directories in a local interactive user's home directory are owned by the user.

Check the owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

ls -lLR /home/smithj -rw-r–r– 1 smithj smithj 18 Mar 5 17:06 file1 -rw-r–r– 1 smithj smithj 193 Mar 5 17:06 file2 -rw-r–r– 1 smithj smithj 231 Mar 5 17:06 file3

If any files are found with an owner different than the home directory user, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72025 - All files and directories contained in local interactive user home directories must be group-owned by a group of which the home directory owner is a member. - RHEL-07-020670

Severity

Medium

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.

Fix

Change the group of a local interactive user's files and directories to a group that the interactive user is a member of. To change the group owner of a local interactive user's files and directories, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

chgrp users /home/smithj/<file>

Check

Verify all files and directories in a local interactive user home directory are group-owned by a group the user is a member of.

Check the group owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

ls -lLR /<home directory>/<users home directory>/ -rw-r–r– 1 smithj smithj 18 Mar 5 17:06 file1 -rw-r–r– 1 smithj smithj 193 Mar 5 17:06 file2 -rw-r–r– 1 smithj sa 231 Mar 5 17:06 file3

If any files are found with an owner different than the group home directory user, check to see if the user is a member of that group with the following command:

grep smithj /etc/group sa:x:100:juan,shelley,bob,smithj smithj:x:521:smithj

If the user is not a member of a group that group owns file(s) in a local interactive user's home directory, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72027 - All files and directories contained in local interactive user home directories must have mode 0750 or less permissive. - RHEL-07-020680

Severity

Medium

Description

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

Fix

Set the mode on files and directories in the local interactive user home directory with the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

chmod 0750 /home/smithj/<file>

Check

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750".

Check the mode of all non-initialization files in a local interactive user home directory with the following command:

Files that begin with a "." are excluded from this requirement.

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

ls -lLR /home/smithj -rwxr-x— 1 smithj smithj 18 Mar 5 17:06 file1 -rwxr—— 1 smithj smithj 193 Mar 5 17:06 file2 -rw-r-x— 1 smithj smithj 231 Mar 5 17:06 file3

If any files are found with a mode more permissive than "0750", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72029 - All local initialization files for interactive users must be owned by the home directory user or root. - RHEL-07-020690

Severity

Medium

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.

Fix

Set the owner of the local initialization files for interactive users to either the directory owner or root with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

chown smithj /home/smithj/.*

Check

Verify all local initialization files for interactive users are owned by the home directory user or root.

Check the owner on all local initialization files with the following command:

Note: The example will be for the "smithj" user, who has a home directory of "/home/smithj".

ls -al /home/smithj/.* | more -rwxr-xr-x 1 smithj users 896 Mar 10 2011 .bash_profile -rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login -rwxr-xr-x 1 smithj users 886 Jan 6 2007 .profile

If any file that sets a local interactive user's environment variables to override the system is not owned by the home directory owner or root, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72031 - Local initialization files for local interactive users must be group-owned by the users primary group or root. - RHEL-07-020700

Severity

Medium

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.

Fix

Change the group owner of a local interactive user's files to the group found in "/etc/passwd" for the user. To change the group owner of a local interactive user home directory, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj", and has a primary group of users.

chgrp users /home/smithj/<file>

Check

Verify the local initialization files of all local interactive users are group-owned by that user's primary Group Identifier (GID).

Check the home directory assignment for all non-privileged users on the system with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj" and a primary group of "users".

cut -d: -f 1,4,6 /etc/passwd | egrep ":[1-4][0-9]{3}" smithj:1000:/home/smithj

grep 1000 /etc/group users:x:1000:smithj,jonesj,jacksons

Note: This may miss interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check the group owner of all local interactive users' initialization files with the following command:

ls -al /home/smithj/.* -rwxr-xr-x 1 smithj users 896 Mar 10 2011 .profile -rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login -rwxr-xr-x 1 smithj users 886 Jan 6 2007 .something

If all local interactive users' initialization files are not group-owned by that user's primary GID, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72033 - All local initialization files must have mode 0740 or less permissive. - RHEL-07-020710

Severity

Medium

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.

Fix

Set the mode of the local initialization files to "0740" with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

chmod 0740 /home/smithj/.<INIT_FILE>

Check

Verify that all local initialization files have a mode of "0740" or less permissive.

Check the mode on all local initialization files with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

ls -al /home/smithj/.* | more -rwxr-xr-x 1 smithj users 896 Mar 10 2011 .profile -rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login -rwxr-xr-x 1 smithj users 886 Jan 6 2007 .something

If any local initialization files have a mode more permissive than "0740", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72035 - All local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory. - RHEL-07-020720

Severity

Medium

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).

Fix

Configure the "/etc/fstab" to use the "nosuid" option on file systems that contain user home directories for interactive users.

Check

Verify that all local interactive user initialization files' executable search path statements do not contain statements that will reference a working directory other than the users' home directory.

Check the executable search path statement for all local interactive user initialization files in the users' home directory with the following commands:

Note: The example will be for the smithj user, which has a home directory of "/home/smithj".

grep -i path /home/smithj/.* /home/smithj/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/bin /home/smithj/.bash_profile:export PATH

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72037 - Local initialization files must not execute world-writable programs. - RHEL-07-020730

Severity

Medium

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.

Fix

Set the mode on files being executed by the local initialization files with the following command:

chmod 0755 <file>

Check

Verify that local initialization files do not execute world-writable programs.

Check the system for world-writable files with the following command:

find / -perm -002 -type f -exec ls -ld { } ; | more

For all files listed, check for their presence in the local initialization files with the following commands:

Note: The example will be for a system that is configured to create users' home directories in the "/home" directory.

grep <file> /home//.

If any local initialization files are found to reference world-writable files, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72039 - All system device files must be correctly labeled to prevent unauthorized modification. - RHEL-07-020900

Severity

Medium

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.

Fix

Run the following command to determine which package owns the device file:

rpm -qf <filename>

The package can be reinstalled from a yum repository using the command:

sudo yum reinstall <packagename>

Alternatively, the package can be reinstalled from trusted media using the command:

sudo rpm -Uvh <packagename>

Check

Verify that all system device files are correctly labeled to prevent unauthorized modification.

List all device files on the system that are incorrectly labeled with the following commands:

Note: Device files are normally found under "/dev", but applications may place device files in other directories and may necessitate a search of the entire system.

#find /dev -context *:device_t:* (-type c -o -type b) -printf "%p %Zn"

#find /dev -context *:unlabeled_t:* (-type c -o -type b) -printf "%p %Zn"

Note: There are device files, such as "/dev/vmci", that are used when the operating system is a host virtual machine. They will not be owned by a user on the system and require the "device_t" label to operate. These device files are not a finding.

If there is output from either of these commands, other than already noted, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72041 - File systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed. - RHEL-07-021000

Severity

Medium

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 setguid files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Fix

Configure the “/etc/fstab” to use the “nosuid” option on file systems that contain user home directories.

Check

Verify file systems that contain user home directories are mounted with the “nosuid” option.

Find the file system(s) that contain the user home directories with the following command:

Note: If a separate file system has not been created for the user home directories (user home directories are mounted under “/”), this is not a finding as the “nosuid” option cannot be used on the “/” system.

cut -d: -f 1,6 /etc/passwd | egrep ”:[1-4][0-9]{3}” smithj:/home/smithj thomasr:/home/thomasr

Check the file systems that are mounted at boot time with the following command:

more /etc/fstab

UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4 rw,relatime,discard,data=ordered,nosuid 0 2

If a file system found in “/etc/fstab” refers to the user home directory file system and it does not have the “nosuid” option set, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-000366

V-72043 - File systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed. - RHEL-07-021010

Severity

Medium

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 “setguid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Fix

Configure the “/etc/fstab” to use the “nosuid” option on file systems that are associated with removable media.

Check

Verify file systems that are used for removable media are mounted with the “nouid” option.

Check the file systems that are mounted at boot time with the following command:

more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat noauto,owner,ro,nosuid 0 0

If a file system found in “/etc/fstab” refers to removable media and it does not have the “nosuid” option set, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-000366

V-72045 - File systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed. - RHEL-07-021020

Severity

Medium

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 “setguid” files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Fix

Configure the “/etc/fstab” to use the “nosuid” option on file systems that are being exported via NFS.

Check

Verify file systems that are being NFS exported are mounted with the “nosuid” option.

Find the file system(s) that contain the directories being exported with the following command:

more /etc/fstab | grep nfs

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid 0 0

If a file system found in “/etc/fstab” refers to NFS and it does not have the “nosuid” option set, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-000366

V-72047 - All world-writable directories must be group-owned by root, sys, bin, or an application group. - RHEL-07-021030

Severity

Medium

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.

Fix

Change the group of the world-writable directories to root with the following command:

chgrp root <directory>

Check

Verify all world-writable directories are group-owned by root, sys, bin, or an application group.

Check the system for world-writable directories with the following command:

Note: The value after -fstype must be replaced with the filesystem type. XFS is used as an example.

find / -perm -002 -xdev -type d -fstype xfs -exec ls -lLd {} ; drwxrwxrwt. 2 root root 40 Aug 26 13:07 /dev/mqueue drwxrwxrwt. 2 root root 220 Aug 26 13:23 /dev/shm drwxrwxrwt. 14 root root 4096 Aug 26 13:29 /tmp

If any world-writable directories are not owned by root, sys, bin, or an application group associated with the directory, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None

- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72049 - The umask must be set to 077 for all local interactive user accounts. - RHEL-07-021040

Severity

Medium

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.

Fix

Remove the umask statement from all local interactive users' initialization files.

If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the Information System Security Officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

Check

Verify that the default umask for all local interactive users is "077".

Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.

Check all local interactive user initialization files for interactive users with the following command:

Note: The example is for a system that is configured to create users home directories in the "/home" directory.

grep -i umask /home//.

If any local interactive user initialization files are found to have a umask statement that has a value less restrictive than "077", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72051 - Cron logging must be implemented. - RHEL-07-021100

Severity

Medium

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.

Fix

Configure "rsyslog" to log all cron messages by adding or updating the following line to "/etc/rsyslog.conf":

cron.* /var/log/cron.log

Note: The line must be added before the following entry if it exists in "/etc/rsyslog.conf":

. ~ # discards everything

Check

Verify that "rsyslog" is configured to log cron events.

Check the configuration of "/etc/rsyslog.conf" for the cron facility with the following command:

Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf".

grep cron /etc/rsyslog.conf cron.* /var/log/cron.log

If the command does not return a response, check for cron logging all facilities by inspecting the "/etc/rsyslog.conf" file:

more /etc/rsyslog.conf

Look for the following entry:

. /var/log/messages

If "rsyslog" is not logging messages for the cron facility or all facilities, this is a finding.

If the entry is in the "/etc/rsyslog.conf" file but is after the entry ".", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72053 - If the cron.allow file exists it must be owned by root. - RHEL-07-021110

Severity

Medium

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.

Fix

Set the owner on the "/etc/cron.allow" file to root with the following command:

chown root /etc/cron.allow

Check

Verify that the "cron.allow" file is owned by root.

Check the owner of the "cron.allow" file with the following command:

l s -al /etc/cron.allow -rw——- 1 root root 6 Mar 5 2011 /etc/cron.allow

If the "cron.allow" file exists and has an owner other than root, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72055 - If the cron.allow file exists it must be group-owned by root. - RHEL-07-021120

Severity

Medium

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.

Fix

Set the group owner on the "/etc/cron.allow" file to root with the following command:

chgrp root /etc/cron.allow

Check

Verify that the "cron.allow" file is group-owned by root.

Check the group owner of the "cron.allow" file with the following command:

ls -al /etc/cron.allow -rw——- 1 root root 6 Mar 5 2011 /etc/cron.allow

If the "cron.allow" file exists and has a group owner other than root, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72057 - Kernel core dumps must be disabled unless needed. - RHEL-07-021300

Severity

Medium

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.

Fix

If kernel core dumps are not required, disable the “kdump” service with the following command:

systemctl disable kdump.service

If kernel core dumps are required, document the need with the ISSO.

Check

Verify that kernel core dumps are disabled unless needed.

Check the status of the “kdump” service with the following command:

systemctl status kdump.service kdump.service - Crash recovery kernel arming

Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled) Active: active (exited) since Wed 2015-08-26 13:08:09 EDT; 43min ago

Main PID: 1130 (code=exited, status=0/SUCCESS)

kernel arming.

If the “kdump” service is active, ask the System Administrator if the use of the service is required and documented with the Information System Security Officer (ISSO).

If the service is active and is not documented, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72073 - The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories. - RHEL-07-021620

Severity

Medium

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.

Fix

Configure the file integrity tool to use FIPS 140-2 cryptographic hashes for validating file and directory contents.

If AIDE is installed, ensure the “sha512” rule is present on all file and directory selection lists.

Check

Verify the file integrity tool is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Note: If RHEL-07-021350 is a finding, this is automatically a finding as the system cannot implement FIPS 140-2 approved cryptographic algorithms and hashes.

Check to see if Advanced Intrusion Detection Environment (AIDE) is installed on the system with the following command:

yum list installed aide

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

If there is no application installed to perform file integrity checks, this is a finding.

Note: AIDE is highly configurable at install time. These commands assume the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

find / -name aide.conf

Check the "aide.conf" file to determine if the "sha512" rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the "sha512" rule follows:

All=p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux /bin All # apply the custom rule to the files in bin /sbin All # apply the same custom rule to the files in sbin

If the "sha512" rule is not being used on all selection lines in the "/etc/aide.conf" file, or another file integrity tool is not using FIPS 140-2 approved cryptographic hashes for validating file contents and directories, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72075 - The system must not allow removable media to be used as the boot loader unless approved. - RHEL-07-021700

Severity

Medium

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).

Fix

Remove alternate methods of booting the system from removable media or document the configuration to boot from removable media with the ISSO.

Check

Verify the system is not configured to use a boot loader on removable media.

Note: GRUB 2 reads its configuration from the "/boot/grub2/grub.cfg" file on traditional BIOS-based machines and from the "/boot/efi/EFI/redhat/grub.cfg" file on UEFI machines.

Check for the existence of alternate boot loader configuration files with the following command:

find / -name grub.cfg /boot/grub2/grub.cfg

If a "grub.cfg" is found in any subdirectories other than "/boot/grub2" and "/boot/efi/EFI/redhat", ask the System Administrator if there is documentation signed by the ISSO to approve the use of removable media as a boot loader.

Check that the grub configuration file has the set root command in each menu entry with the following commands:

grep -c menuentry /boot/grub2/grub.cfg 1 # grep 'set root' /boot/grub2/grub.cfg set root=(hd0,1)

If the system is using an alternate boot loader on removable media, and documentation does not exist approving the alternate configuration, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72081 - The 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. - RHEL-07-030010

Severity

Medium

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

Fix

Configure the operating system to shut down in the event of an audit processing failure.

Add or correct the option to shut down the operating system with the following command:

auditctl -f 2

If availability has been determined to be more important, and this decision is documented with the ISSO, configure the operating system to notify system administration staff and ISSO staff in the event of an audit processing failure with the following command:

auditctl -f 1

Kernel log monitoring must also be configured to properly alert designated staff.

The audit daemon must be restarted for the changes to take effect.

Check

Confirm the audit configuration regarding how auditing processing failures are handled.

Check to see what level “auditctl” is set to with following command:

 # auditctl -l | grep /-f -f 2

If the value of "-f" is set to "2", the system is configured to panic (shut down) in the event of an auditing failure.

If the value of "-f" is set to "1", the system is configured to only send information to the kernel log regarding the failure.

If the "-f" flag is not set, this is a CAT I finding.

If the "-f" flag is set to any value other than "1" or "2", this is a CAT II finding.

If the "-f" flag is set to "1" but the availability concern is not documented or there is no monitoring of the kernel log, this is a CAT III finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000139

V-72083 - The operating system must off-load audit records onto a different system or media from the system being audited. - RHEL-07-030300

Severity

Medium

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

Fix

Configure the operating system to off-load audit records onto a different system or media from the system being audited.

Set the remote server option in "/etc/audisp/audisp-remote.conf" with the IP address of the log aggregation server.

Check

Verify the operating system off-loads audit records onto a different system or media from the system being audited.

To determine the remote server that the records are being sent to, use the following command:

grep -i remote_server /etc/audisp/audisp-remote.conf remote_server = 10.0.21.1

If a remote server is not configured, or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the audit logs are being off-loaded to another system or media, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001851

V-72085 - The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited. - RHEL-07-030310

Severity

Medium

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

Fix

Configure the operating system to encrypt the transfer of off-loaded audit records onto a different system or media from the system being audited.

Uncomment the “enable_krb5” option in “/etc/audisp/audisp-remote.conf” and set it with the following line:

enable_krb5 = yes

Check

Verify the operating system encrypts audit records off-loaded onto a different system or media from the system being audited.

To determine if the transfer is encrypted, use the following command:

grep -i enable_krb5 /etc/audisp/audisp-remote.conf enable_krb5 = yes

If the value of the “enable_krb5” option is not set to “yes” or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001851

V-72087 - The audit system must take appropriate action when the audit storage volume is full. - RHEL-07-030320

Severity

Medium

Description

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

Fix

Configure the action the operating system takes if the disk the audit records are written to becomes full.

Uncomment or edit the “disk_full_action” option in “/etc/audisp/audisp-remote.conf” and set it to “syslog”, “single”, or “halt”, such as the following line:

disk_full_action = single

Uncomment the “network_failure_action” option in “/etc/audisp/audisp-remote.conf” and set it to “syslog”, “single”, or “halt”.

Check

Verify the action the operating system takes if the disk the audit records are written to becomes full.

To determine the action that takes place if the disk is full on the remote server, use the following command:

grep -i disk_full_action /etc/audisp/audisp-remote.conf disk_full_action = single

To determine the action that takes place if the network connection fails, use the following command:

grep -i network_failure_action /etc/audisp/audisp-remote.conf network_failure_action = stop

If the value of the “network_failure_action” option is not “syslog”, “single”, or “halt”, or the line is commented out, this is a finding.

If the value of the “disk_full_action” option is not “syslog”, “single”, or “halt”, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001851

V-72089 - The operating system must immediately 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. - RHEL-07-030330

Severity

Medium

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.

Fix

Configure the operating system to immediately notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Check the system configuration to determine the partition the audit records are being written to:

grep log_file /etc/audit/auditd.conf

Determine the size of the partition that audit records are written to (with the example being "/var/log/audit/"):

df -h /var/log/audit/

Set the value of the "space_left" keyword in "/etc/audit/auditd.conf" to 75 percent of the partition size.

Check

Verify the operating system immediately notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Check the system configuration to determine the partition the audit records are being written to with the following command:

grep log_file /etc/audit/auditd.conf log_file = /var/log/audit/audit.log

Check the size of the partition that audit records are written to (with the example being "/var/log/audit/"):

df -h /var/log/audit/ 0.9G /var/log/audit

If the audit records are not being written to a partition specifically created for audit records (in this example "/var/log/audit" is a separate partition), determine the amount of space other files in the partition are currently occupying with the following command:

du -sh <partition> 1.8G /var

Determine what the threshold is for the system to take action when 75 percent of the repository maximum audit record storage capacity is reached:

grep -i space_left /etc/audit/auditd.conf space_left = 225

If the value of the "space_left" keyword is not set to 25 percent of the total partition size, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001855

V-72091 - The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached. - RHEL-07-030340

Severity

Medium

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.

Fix

Configure the operating system to immediately notify the SA and ISSO (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Uncomment or edit the “space_left_action” keyword in “/etc/audit/auditd.conf” and set it to “email”.

space_left_action = email

Check

Verify the operating system immediately notifies the SA and ISSO (at a minimum) via email when the allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Check what action the operating system takes when the threshold for the repository maximum audit record storage capacity is reached with the following command:

grep -i space_left_action /etc/audit/auditd.conf space_left_action = email

If the value of the “space_left_action” keyword is not set to “email”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001855

V-72093 - The 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. - RHEL-07-030350

Severity

Medium

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.

Fix

Configure the operating system to immediately notify the SA and ISSO (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Uncomment or edit the “action_mail_acct” keyword in “/etc/audit/auditd.conf” and set it to root and any other accounts associated with security personnel.

action_mail_acct = root

Check

Verify the operating system immediately notifies the SA and ISSO (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached.

Check what account the operating system emails when the threshold for the repository maximum audit record storage capacity is reached with the following command:

grep -i action_mail_acct /etc/audit/auditd.conf action_mail_acct = root

If the value of the "action_mail_acct" keyword is not set to "root" and other accounts for security personnel, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001855

V-72095 - All privileged function executions must be audited. - RHEL-07-030360

Severity

Medium

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.

Fix

Configure the operating system to audit the execution of privileged functions.

To find the relevant “setuid”/”setgid” programs, run the following command for each local partition [PART]:

find [PART] -xdev -type f (-perm -4000 -o -perm -2000) 2>/dev/null

For each “setuid”/”setgid” program on the system, which is not covered by an audit rule for a (sub) directory (such as “/usr/sbin”), add a line of the following form to “/etc/audit/audit.rules”, where <suid_prog_with_full_path> is the full path to each “setuid”/”setgid” program in the list:

-a always,exit -F <suid_prog_with_full_path> -F perm=x -F auid>=1000 -F auid!=4294967295 -k setuid/setgid

Check

Verify the operating system audits the execution of privileged functions.

To find relevant setuid and setgid programs, use the following command once for each local partition [PART]:

find [PART] -xdev -type f (-perm -4000 -o -perm -2000) 2>/dev/null

Run the following command to verify entries in the audit rules for all programs found with the previous command:

grep <suid_prog_with_full_path> -a always,exit -F <suid_prog_with_full_path> -F perm=x -F auid>=1000 -F auid!=4294967295 -k setuid/setgid

All “setuid” and “setgid” files on the system must have a corresponding audit rule, or must have an audit rule for the (sub) directory that contains the “setuid”/”setgid” file.

If all “setuid”/”setgid” files on the system do not have audit rule coverage, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002234

V-72097 - All uses of the chown command must be audited. - RHEL-07-030370

Severity

Medium

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

Fix

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chown" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i chown /etc/audit/audit.rules

-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172

V-72099 - All uses of the fchown command must be audited. - RHEL-07-030380

Severity

Medium

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

Fix

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "fchown" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i fchown /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172

V-72101 - All uses of the lchown command must be audited. - RHEL-07-030390

Severity

Medium

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

Fix

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "lchown" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i lchown /etc/audit/audit.rules

-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172

V-72103 - All uses of the fchownat command must be audited. - RHEL-07-030400

Severity

Medium

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

Fix

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "fchownat" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i fchownat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172

V-72105 - All uses of the chmod command must be audited. - RHEL-07-030410

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "chmod" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chmod" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i chmod /etc/audit/audit.rules

-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72107 - All uses of the fchmod command must be audited. - RHEL-07-030420

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "fchmod" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "fchmod" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i fchmod /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-000172

V-72109 - All uses of the fchmodat command must be audited. - RHEL-07-030430

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "fchmodat" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "fchmodat" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i fchmodat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72111 - All uses of the setxattr command must be audited. - RHEL-07-030440

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "setxattr" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "setxattr" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i setxattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72113 - All uses of the fsetxattr command must be audited. - RHEL-07-030450

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "fsetxattr" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "fsetxattr" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i fsetxattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72115 - All uses of the lsetxattr command must be audited. - RHEL-07-030460

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "lsetxattr" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "lsetxattr" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i lsetxattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-000172

V-72117 - All uses of the removexattr command must be audited. - RHEL-07-030470

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "removexattr" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "removexattr" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i removexattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72119 - All uses of the fremovexattr command must be audited. - RHEL-07-030480

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "fremovexattr" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "fremovexattr" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i fremovexattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72121 - All uses of the lremovexattr command must be audited. - RHEL-07-030490

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "lremovexattr" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "lremovexattr" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i lremovexattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72123 - All uses of the creat command must be audited. - RHEL-07-030500

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "creat" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "creat" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i creat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S creat -Fexit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72125 - All uses of the open command must be audited. - RHEL-07-030510

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "open" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S open -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "open" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i open /etc/audit/audit.rules

-a always,exit -F arch=b32 -S open -Fexit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72127 - All uses of the openat command must be audited. - RHEL-07-030520

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "openat" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "openat" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i openat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S openat -Fexit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72129 - All uses of the open_by_handle_at command must be audited. - RHEL-07-030530

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "open_by_handle_at" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "open_by_handle_at" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i open_by_handle_at /etc/audit/audit.rules

-a always,exit -F arch=b32 -S open_by_handle_at -Fexit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72131 - All uses of the truncate command must be audited. - RHEL-07-030540

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "truncate" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "truncate" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i truncate /etc/audit/audit.rules

-a always,exit -F arch=b32 -S truncate -Fexit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72133 - All uses of the ftruncate command must be audited. - RHEL-07-030550

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "ftruncate" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "ftruncate" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i ftruncate /etc/audit/audit.rules

-a always,exit -F arch=b32 -S ftruncate -Fexit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72135 - All uses of the semanage command must be audited. - RHEL-07-030560

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “semanage” command occur.

Add or update the following rule in “/etc/audit/rules.d/audit.rules”:

-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "semanage" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/sbin/semanage /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72137 - All uses of the setsebool command must be audited. - RHEL-07-030570

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "setsebool" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "setsebool" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/sbin/setsebool /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72139 - All uses of the chcon command must be audited. - RHEL-07-030580

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "chcon" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chcon" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/bin/chcon /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72141 - All uses of the restorecon command must be audited. - RHEL-07-030590

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "restorecon" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/sbin/restorecon -F perm=x -F auid>=1000 -F auid!=4294967295 -k -F privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "restorecon" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/sbin/restorecon /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/restorecon -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72143 - The operating system must generate audit records for all successful/unsuccessful account access count events. - RHEL-07-030600

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful account access count events occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-w /var/log/tallylog -p wa -k logins

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful account access count events occur.

Check the file system rule in "/etc/audit/audit.rules" with the following commands:

grep -i /var/log/tallylog /etc/audit/audit.rules

-w /var/log/tallylog -p wa -k logins

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None

- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172, CCI-002884

V-72145 - The operating system must generate audit records for all unsuccessful account access events. - RHEL-07-030610

Severity

Medium

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

Fix

Configure the operating system to generate audit records when unsuccessful account access events occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-w /var/run/faillock/ -p wa -k logins

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when unsuccessful account access events occur.

Check the file system rule in "/etc/audit/audit.rules" with the following commands:

grep -i /var/run/faillock /etc/audit/audit.rules

-w /var/run/faillock -p wa -k logins

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None

- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172, CCI-002884

V-72147 - The operating system must generate audit records for all successful account access events. - RHEL-07-030620

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful account access events occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-w /var/log/lastlog -p wa -k logins

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful account access events occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

grep -i /var/log/lastlog /etc/audit/audit.rules

-w /var/log/lastlog -p wa -k logins

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000126, CCI-000172, CCI-002884

V-72149 - All uses of the passwd command must be audited. - RHEL-07-030630

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “passwd” command occur.

Add or update the following rule in “/etc/audit/rules.d/audit.rules”:

-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "passwd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/bin/passwd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72151 - All uses of the unix_chkpwd command must be audited. - RHEL-07-030640

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "unix_chkpwd" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "unix_chkpwd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /sbin/unix_chkpwd /etc/audit/audit.rules

-a always,exit -F path=/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72153 - All uses of the gpasswd command must be audited. - RHEL-07-030650

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "gpasswd" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "gpasswd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/bin/gpasswd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72155 - All uses of the chage command must be audited. - RHEL-07-030660

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "chage" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chage" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/bin/chage /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72157 - All uses of the userhelper command must be audited. - RHEL-07-030670

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "userhelper" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "userhelper" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

grep -i /usr/sbin/userhelper /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72159 - All uses of the su command must be audited. - RHEL-07-030680

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "su" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "su" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /bin/su /etc/audit/audit.rules

-a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000130, CCI-000135, CCI-000172, CCI-002884

V-72161 - All uses of the sudo command must be audited. - RHEL-07-030690

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “sudo” command occur.

Add or update the following rule in “/etc/audit/rules.d/audit.rules”:

-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "sudo" command occur.

Check for the following system calls being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/bin/sudo /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000130, CCI-000135, CCI-000172, CCI-002884

V-72163 - All uses of the sudoers command must be audited. - RHEL-07-030700

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "sudoer" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-w /etc/sudoers -p wa -k privileged-actions

-w /etc/sudoers.d -p wa -k privileged-actions

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "sudoer" command occur.

Check for modification of the following files being audited by performing the following commands to check the file system rules in "/etc/audit/audit.rules":

grep /etc/sudoers /etc/audit/audit.rules

-w /etc/sudoers -p wa -k privileged-actions

grep /etc/sudoers.d /etc/audit/audit.rules

-w /etc/sudoers.d -p wa -k privileged-actions

If the commands do not return output that does not match the examples, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000130, CCI-000135, CCI-000172, CCI-002884

V-72165 - All uses of the newgrp command must be audited. - RHEL-07-030710

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "newgrp" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "newgrp" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/bin/newgrp /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000130, CCI-000135, CCI-000172, CCI-002884

V-72167 - All uses of the chsh command must be audited. - RHEL-07-030720

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “chsh” command occur.

Add or update the following rule in “/etc/audit/rules.d/audit.rules”:

-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the “chsh” command occur.

Check for the following system call being audited by performing the following command to check the file system rules in “/etc/audit/audit.rules”:

grep -i /usr/bin/chsh /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None

- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000130, CCI-000135, CCI-000172, CCI-002884

V-72169 - All uses of the sudoedit command must be audited. - RHEL-07-030730

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "sudoedit" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/bin/sudoedit -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "sudoedit" command occur.

Check for the following system calls being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/bin/sudoedit /etc/audit/audit.rules

-a always,exit -F path=/bin/sudoedit -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None

- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000130, CCI-000135, CCI-000172, CCI-002884

V-72171 - All uses of the mount command must be audited. - RHEL-07-030740

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "mount" command occur.

Add or update the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount

-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "mount" command occur.

Check for the following system calls being audited by performing the following series of commands to check the file system rules in "/etc/audit/audit.rules":

grep -i /bin/mount /etc/audit/audit.rules

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount

-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-002884

V-72173 - All uses of the umount command must be audited. - RHEL-07-030750

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “umount” command occur.

Add or update the following rule in “/etc/audit/rules.d/audit.rules”:

-a always,exit -F path=/bin/umount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-mount

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "umount" command occur.

Check for the following system calls being audited by performing the following series of commands to check the file system rules in "/etc/audit/audit.rules":

grep -i /bin/umount /etc/audit/audit.rules

-a always,exit -F path=/bin/umount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-mount

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-002884

V-72175 - All uses of the postdrop command must be audited. - RHEL-07-030760

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "postdrop" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-postfix

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "postdrop" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/sbin/postdrop /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-postfix

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-002884

V-72177 - All uses of the postqueue command must be audited. - RHEL-07-030770

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "postqueue" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-postfix

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "postqueue" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/sbin/postqueue /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-postfix

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-002884

V-72179 - All uses of the ssh-keysign command must be audited. - RHEL-07-030780

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "ssh-keysign" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-ssh

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "ssh-keysign" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/libexec/openssh/ssh-keysign /etc/audit/audit.rules

-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-ssh

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72181 - All uses of the pt_chown command must be audited. - RHEL-07-030790

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "pt_chown" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/libexec/pt_chown -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged_terminal

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "pt_chown" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/libexec/pt_chown /etc/audit/audit.rules

-a always,exit -F path=/usr/libexec/pt_chown -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged_terminal

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72183 - All uses of the crontab command must be audited. - RHEL-07-030800

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “crontab” command occur.

Add or update the following rule in “/etc/audit/rules.d/audit.rules”:

-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-cron

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "crontab" command occur.

Check for the following system call being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

grep -i /usr/bin/crontab /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-cron

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000135, CCI-000172, CCI-002884

V-72185 - All uses of the pam_timestamp_check command must be audited. - RHEL-07-030810

Severity

Medium

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.

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "pam_timestamp_check" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/sbin/pam_timestamp_check -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-pam

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "pam_timestamp_check" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep -i /sbin/pam_timestamp_check /etc/audit/audit.rules

-a always,exit -F path=/sbin/pam_timestamp_check -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-pam

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72187 - All uses of the init_module command must be audited. - RHEL-07-030820

Severity

Medium

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

Fix

Configure the operating system generates audit records when successful/unsuccessful attempts to use the "init_module" command occur.

Add or update the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S init_module -k module-change

-a always,exit -F arch=b64 -S init_module -k module-change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "init_module" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

grep -i init_module /etc/audit/audit.rules

If the command does not return the following output (appropriate to the architecture), this is a finding.

-a always,exit -F arch=b32 -S init_module -k module-change

-a always,exit -F arch=b64 -S init_module -k module-change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72189 - All uses of the delete_module command must be audited. - RHEL-07-030830

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "delete_module" command occur.

Add or update the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S delete_module -k module-change

-a always,exit -F arch=b64 -S delete_module -k module-change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "delete_module" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

grep -i delete_module /etc/audit/audit.rules

If the command does not return the following output (appropriate to the architecture), this is a finding.

-a always,exit -F arch=b32 -S delete_module -k module-change

-a always,exit -F arch=b64 -S delete_module -k module-change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72191 - All uses of the insmod command must be audited. - RHEL-07-030840

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "insmod" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-w /sbin/insmod -p x -F auid!=4294967295 -k module-change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "insmod" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep -i insmod /etc/audit/audit.rules

If the command does not return the following output (appropriate to the architecture), this is a finding.

-w /sbin/insmod -p x -F auid!=4294967295 -k module-change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72193 - All uses of the rmmod command must be audited. - RHEL-07-030850

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "rmmod" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-w /sbin/rmmod-p x -F auid!=4294967295 -k module-change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "rmmod" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep -i rmmod /etc/audit/audit.rules

If the command does not return the following output (appropriate to the architecture), this is a finding.

-w /sbin/rmmod -p x -F auid!=4294967295 -k module-change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72195 - All uses of the modprobe command must be audited. - RHEL-07-030860

Severity

Medium

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

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "modprobe" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-w /sbin/modprobe -p x -F auid!=4294967295 -k module-change

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "modprobe" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

grep -i modprobe /etc/audit/audit.rules

If the command does not return the following output (appropriate to the architecture), this is a finding.

-w /sbin/modprobe -p x -F auid!=4294967295 -k module-change

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172

V-72197 - The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. - RHEL-07-030870

Severity

Medium

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

Fix

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Add or update the following rule "/etc/audit/rules.d/audit.rules":

-w /etc/passwd -p wa -k identity

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep /etc/passwd /etc/audit/audit.rules

-w /etc/passwd -p wa -k audit_rules_usergroup_modification

If the command does not return a line, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000018, CCI-000172, CCI-001403, CCI-002130

V-72199 - All uses of the rename command must be audited. - RHEL-07-030880

Severity

Medium

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.

Satisfies: SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "rename" command occur.

Add the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S rename -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S rename -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "rename" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i rename /etc/audit/audit.rules -a always,exit -F arch=b32 -S rename -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S rename -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72201 - All uses of the renameat command must be audited. - RHEL-07-030890

Severity

Medium

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.

Satisfies: SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the “renameat” command occur.

Add the following rules in “/etc/audit/rules.d/audit.rules” (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S renameat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S renameat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "renameat" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i renameat /etc/audit/audit.rules -a always,exit -F arch=b32 -S renameat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S renameat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72203 - All uses of the rmdir command must be audited. - RHEL-07-030900

Severity

Medium

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.

Satisfies: SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "rmdir" command occur.

Add the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S rmdir -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S rmdir -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "rmdir" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i rmdir /etc/audit/audit.rules -a always,exit -F arch=b32 -S rmdir -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S rmdir -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72205 - All uses of the unlink command must be audited. - RHEL-07-030910

Severity

Medium

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.

Satisfies: SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "unlink" command occur.

Add the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S unlink -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S unlink -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "unlink" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i unlink/etc/audit/audit.rules -a always,exit -F arch=b32 -S unlink -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S unlink -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72207 - All uses of the unlinkat command must be audited. - RHEL-07-030920

Severity

Medium

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.

Satisfies: SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172

Fix

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "unlinkat" command occur.

Add the following rules in "/etc/audit/rules.d/audit.rules" (removing those that do not match the CPU architecture):

-a always,exit -F arch=b32 -S unlinkat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S unlinkat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "unlinkat" command occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

grep -i unlinkat/etc/audit/audit.rules -a always,exit -F arch=b32 -S unlinkat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete -a always,exit -F arch=b64 -S unlinkat -F perm=x -F auid>=1000 -F auid!=4294967295 -k delete

If the command does not return any output, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000172, CCI-002884

V-72209 - The system must send rsyslog output to a log aggregation server. - RHEL-07-031000

Severity

Medium

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.

Fix

Modify the "/etc/rsyslog.conf" file to contain a configuration line to send all "rsyslog" output to a log aggregation system:

. @@<log aggregation system name>

Check

Verify "rsyslog" is configured to send all messages to a log aggregation server.

Check the configuration of "rsyslog" with the following command:

Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf".

grep @ /etc/rsyslog.conf . @@logagg.site.mil

If there are no lines in the "/etc/rsyslog.conf" file that contain the "@" or "@@" symbol(s), and the lines with the correct symbol(s) to send output to another system do not cover all "rsyslog" output, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the audit logs are being sent to another system, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72211 - The rsyslog daemon must not accept log messages from other servers unless the server is being used for log aggregation. - RHEL-07-031010

Severity

Medium

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.

Fix

Modify the "/etc/rsyslog.conf" file to remove the "ModLoad imtcp" configuration line, or document the system as being used for log aggregation.

Check

Verify that the system is not accepting "rsyslog" messages from other systems unless it is documented as a log aggregation server.

Check the configuration of "rsyslog" with the following command:

grep imtcp /etc/rsyslog.conf ModLoad imtcp

If the "imtcp" module is being loaded in the "/etc/rsyslog.conf" file, ask to see the documentation for the system being used for log aggregation.

If the documentation does not exist, or does not specify the server as a log aggregation system, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72215 - The system must update the DoD-approved virus scan program every seven days or more frequently. - RHEL-07-032010

Severity

Medium

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 check for software and virus definition updates with a frequency no longer than seven days. If a manual process is required to update the virus scan software or definitions, it must be documented with the Information System Security Officer (ISSO).

Fix

Update the approved DoD virus scan software and virus definition files.

Check

Verify the system is using a DoD-approved virus scan program and the virus definition file is less than seven days old.

Check for the presence of "McAfee VirusScan Enterprise for Linux" with the following command:

systemctl status nails nails - service for McAfee VirusScan Enterprise for Linux > Loaded: loaded /opt/NAI/package/McAfeeVSEForLinux/McAfeeVSEForLinux-2.0.2.<build_number>; enabled) > Active: active (running) since Mon 2015-09-27 04:11:22 UTC;21 min ago

If the "nails" service is not active, check for the presence of "clamav" on the system with the following command:

systemctl status clamav-daemon.socket systemctl status clamav-daemon.socket

clamav-daemon.socket - Socket for Clam AntiVirus userspace daemon Loaded: loaded (/lib/systemd/system/clamav-daemon.socket; enabled) Active: active (running) since Mon 2015-01-12 09:32:59 UTC; 7min ago

If “McAfee VirusScan Enterprise for Linux” is active on the system, check the dates of the virus definition files with the following command:

ls -al /opt/NAI/LinuxShield/engine/dat/*.dat <need output>

If the virus definition files have dates older than seven days from the current date, this is a finding.

If “clamav” is active on the system, check the dates of the virus database with the following commands:

grep -I databasedirectory /etc/clamav.conf DatabaseDirectory /var/lib/clamav

ls -al /var/lib/clamav/*.cvd -rwxr-xr-x 1 root root 149156 Mar 5 2011 daily.cvd

If the database file has a date older than seven days from the current date, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001668

V-72219 - The host 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. - RHEL-07-040100

Severity

Medium

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

Fix

Update the host's firewall settings and/or running services to comply with the PPSM CLSA for the site or program and the PPSM CAL.

Check

Inspect the firewall configuration and running services to verify that it is configured to prohibit or restrict the use of functions, ports, protocols, and/or services that are unnecessary or prohibited.

Check which services are currently active with the following command:

firewall-cmd –list-all public (default, active)

> interfaces: enp0s3 sources: services: dhcpv6-client dns http https ldaps rpc-bind ssh ports: masquerade: no forward-ports: icmp-blocks: rich rules:

Ask the System Administrator for the site or program PPSM CLSA. Verify the services allowed by the firewall match the PPSM CLSA.

If there are additional ports, protocols, or services that are not in the PPSM CLSA, or there are ports, protocols, or services that are prohibited by the PPSM Category Assurance List (CAL), this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000382, CCI-002314

V-72221 - A FIPS 140-2 approved cryptographic algorithm must be used for SSH communications. - RHEL-07-040110

Severity

Medium

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

Fix

Configure SSH to use FIPS 140-2 approved cryptographic algorithms.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).

Ciphers aes128-ctr,aes192-ctr,aes256-ctr

The SSH service must be restarted for changes to take effect.

Check

Verify the operating system uses mechanisms meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Note: If RHEL-07-021350 is a finding, this is automatically a finding as the system cannot implement FIPS 140-2-approved cryptographic algorithms and hashes.

The location of the "sshd_config" file may vary if a different daemon is in use.

Inspect the "Ciphers" configuration with the following command:

grep -i ciphers /etc/ssh/sshd_config Ciphers aes128-ctr,aes192-ctr,aes256-ctr

If any ciphers other than "aes128-ctr", "aes192-ctr", or "aes256-ctr" are listed, the "Ciphers" keyword is missing, or the retuned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None

- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000068, CCI-000366, CCI-000803

V-72223 - All network connections associated with a communication session must be 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. - RHEL-07-040160

Severity

Medium

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.

Fix

Configure the operating system to terminate all network connections associated with a communications session at the end of the session or after a period of inactivity.

Add the following line to "/etc/profile" (or modify the line to have the required value):

TMOUT=600

The SSH service must be restarted for changes to take effect.

Check

Verify the operating system terminates all network connections associated with a communications session at the end of the session or based on inactivity.

Check the value of the system inactivity timeout with the following command:

grep -i tmout /etc/bashrc TMOUT=600

If “TMOUT” is not set to “600” or less in “/etc/bashrc”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001133, CCI-002361

V-72225 - The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts. - RHEL-07-040170

Severity

Medium

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

Fix

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via the ssh.

Edit the "/etc/ssh/sshd_config" file to uncomment the banner keyword and configure it to point to a file that will contain the logon banner (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). An example configuration line is:

banner=/etc/issue

Either create the file containing the banner or replace the text in the file with the Standard Mandatory DoD Notice and Consent Banner. The DoD required text is:

"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."

The SSH service must be restarted for changes to take effect.

Check

Verify any publicly accessible connection to the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Check for the location of the banner file being used with the following command:

grep -i banner /etc/ssh/sshd_config

banner=/etc/issue

This command will return the banner keyword and the name of the file that contains the ssh banner (in this case "/etc/issue").

If the line is commented out, this is a finding.

View the file specified by the banner keyword to check that it matches the text of the Standard Mandatory DoD Notice and Consent Banner:

"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."

If the system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

If the text in the file does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000048, CCI-000050, CCI-001384, CCI-001385, CCI-001386, CCI-001387, CCI-001388

V-72227 - The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications. - RHEL-07-040180

Severity

Medium

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.

Fix

Configure the operating system to implement cryptography to protect the integrity of LDAP authentication sessions.

Set the USELDAPAUTH=yes in "/etc/sysconfig/authconfig".

Set "ssl start_tls" in "/etc/pam_ldap.conf".

Check

Verify the operating system implements cryptography to protect the integrity of remote LDAP authentication sessions.

To determine if LDAP is being used for authentication, use the following command:

grep -i useldapauth /etc/sysconfig/authconfig USELDAPAUTH=yes

If USELDAPAUTH=yes, then LDAP is being used. To see if LDAP is configured to use TLS, use the following command:

grep -i ssl /etc/pam_ldap.conf ssl start_tls

If the "ssl" option is not "start_tls", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None

- Third Party Tools: None
- Control Correlation Identifiers: CCI-001453

V-72229 - The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. - RHEL-07-040190

Severity

Medium

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.

Fix

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.

Set the "tls_cacertdir" option in "/etc/pam_ldap.conf" to point to the directory that will contain the X.509 certificates for peer authentication.

Set the "tls_cacertfile" option in "/etc/pam_ldap.conf" to point to the path for the X.509 certificates used for peer authentication.

Check

Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.

To determine if LDAP is being used for authentication, use the following command:

grep -i useldapauth /etc/sysconfig/authconfig USELDAPAUTH=yes

If USELDAPAUTH=yes, then LDAP is being used.

Check for the directory containing X.509 certificates for peer authentication with the following command:

grep -i cacertdir /etc/pam_ldap.conf tls_cacertdir /etc/openldap/certs

Verify the directory set with the "tls_cacertdir" option exists.

If the directory does not exist or the option is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001453

V-72231 - The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications. - RHEL-07-040200

Severity

Medium

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.

Fix

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.

Set the “tls_cacertfile” option in “/etc/pam_ldap.conf” to point to the path for the X.509 certificates used for peer authentication.

Check

Verify the operating system implements cryptography to protect the integrity of remote ldap access sessions.

To determine if LDAP is being used for authentication, use the following command:

grep -i useldapauth /etc/sysconfig/authconfig USELDAPAUTH=yes

If USELDAPAUTH=yes, then LDAP is being used.

Check that the path to the X.509 certificate for peer authentication with the following command:

grep -i cacertfile /etc/pam_ldap.conf tls_cacertfile /etc/openldap/ldap-cacert.pem

Verify the "tls_cacertfile" option points to a file that contains the trusted CA certificate.

If this file does not exist, or the option is commented out or missing, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001453

V-72233 - All networked systems must have SSH installed. - RHEL-07-040300

Severity

Medium

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

Fix

Install SSH packages onto the host with the following commands:

yum install openssh-clients.x86_64 # yum install openssh-server.x86_64

Note: 32-bit versions will require different packages.

Check

Check to see if sshd is installed with the following command:

yum list installed ssh libssh2.x86_64 1.4.3-8.el7 @anaconda/7.1 openssh.x86_64 6.6.1p1-11.el7 @anaconda/7.1 openssh-clients.x86_64 6.6.1p1-11.el7 @anaconda/7.1 openssh-server.x86_64 6.6.1p1-11.el7 @anaconda/7.1

If the “SSH server” package is not installed, this is a finding.

If the “SSH client” package is not installed, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002418, CCI-002420, CCI-002421, CCI-002422

V-72235 - All networked systems must use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission. - RHEL-07-040310

Severity

Medium

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

Fix

Configure the SSH service to automatically start after reboot with the following command:

systemctl enable sshd ln -s '/usr/lib/systemd/system/sshd.service' '/etc/systemd/system/multi-user.target.wants/sshd.service'

Check

Verify SSH is loaded and active with the following command:

 # systemctl status sshd

sshd.service - OpenSSH server daemon Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled) Active: active (running) since Tue 2015-11-17 15:17:22 EST; 4 weeks 0 days ago

Main PID: 1348 (sshd)

CGroup: /system.slice/sshd.service ??1348 /usr/sbin/sshd -D

If "sshd" does not show a status of "active" and "running", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-002418, CCI-002420, CCI-002421, CCI-002422

V-72237 - All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements. - RHEL-07-040320

Severity

Medium

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

Fix

Configure the operating system to automatically terminate a user session after inactivity time-outs have expired or at shutdown.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

ClientAliveInterval 600

The SSH service must be restarted for changes to take effect.

Check

Verify the operating system automatically terminates a user session after inactivity time-outs have expired.

Check for the value of the "ClientAlive" keyword with the following command:

grep -i clientalive /etc/ssh/sshd_config

ClientAliveInterval 600

If "ClientAliveInterval" is not set to "600" in "/etc/ ssh/sshd_config", and a lower value is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001133, CCI-002361

V-72239 - The SSH daemon must not allow authentication using RSA rhosts authentication. - RHEL-07-040330

Severity

Medium

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.

Fix

Configure the SSH daemon to not allow authentication using RSA rhosts authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

RhostsRSAAuthentication yes

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon does not allow authentication using RSA rhosts authentication.

To determine how the SSH daemon's "RhostsRSAAuthentication" option is set, run the following command:

grep RhostsRSAAuthentication /etc/ssh/sshd_config

RhostsRSAAuthentication yes

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72241 - All network connections associated with SSH traffic must terminate after a period of inactivity. - RHEL-07-040340

Severity

Medium

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

Fix

Configure the operating system to automatically terminate a user session after inactivity time-outs have expired or at shutdown.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

ClientAliveCountMax 0

The SSH service must be restarted for changes to take effect.

Check

Verify the operating system automatically terminates a user session after inactivity time-outs have expired.

Check for the value of the "ClientAliveCountMax" keyword with the following command:

grep -i clientalivecount /etc/ssh/sshd_config ClientAliveCountMax 0

If "ClientAliveCountMax" is not set to "0" in "/etc/ ssh/sshd_config", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001133, CCI-002361

V-72243 - The SSH daemon must not allow authentication using rhosts authentication. - RHEL-07-040350

Severity

Medium

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.

Fix

Configure the SSH daemon to not allow authentication using known hosts authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

IgnoreRhosts yes

Check

Verify the SSH daemon does not allow authentication using known hosts authentication.

To determine how the SSH daemon's "IgnoreRhosts" option is set, run the following command:

grep -i IgnoreRhosts /etc/ssh/sshd_config

IgnoreRhosts yes

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72245 - The system must display the date and time of the last successful account logon upon an SSH logon. - RHEL-07-040360

Severity

Medium

Description

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Fix

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/sshd" or in the "sshd_config" file used by the system ("/etc/ssh/sshd_config" will be used in the example) (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).

Add the following line to the top of "/etc/pam.d/sshd":

session required pam_lastlog.so showfailed

Or modify the "PrintLastLog" line in "/etc/ssh/sshd_config" to match the following:

PrintLastLog yes

The SSH service must be restarted for changes to "sshd_config" to take effect.

Check

Verify SSH provides users with feedback on when account accesses last occurred.

Check that "PrintLastLog" keyword in the sshd daemon configuration file is used and set to "yes" with the following command:

grep -i printlastlog /etc/ssh/sshd_config PrintLastLog yes

If the "PrintLastLog" keyword is set to "no", is missing, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72247 - The system must not permit direct logons to the root account using remote access via SSH. - RHEL-07-040370

Severity

Medium

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.

Fix

Configure SSH to stop users from logging on remotely as the root user.

Edit the appropriate "/etc/ssh/sshd_config" file to uncomment or add the line for the "PermitRootLogin" keyword and set its value to "no" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

PermitRootLogin no

The SSH service must be restarted for changes to take effect.

Check

Verify remote access using SSH prevents users from logging on directly as root.

Check that SSH prevents users from logging on directly as root with the following command:

grep -i permitrootlogin /etc/ssh/sshd_config PermitRootLogin no

If the "PermitRootLogin" keyword is set to "yes", is missing, or is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72249 - The SSH daemon must not allow authentication using known hosts authentication. - RHEL-07-040380

Severity

Medium

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.

Fix

Configure the SSH daemon to not allow authentication using known hosts authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

IgnoreUserKnownHosts yes

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon does not allow authentication using known hosts authentication.

To determine how the SSH daemon's "IgnoreUserKnownHosts" option is set, run the following command:

grep -i IgnoreUserKnownHosts /etc/ssh/sshd_config

IgnoreUserKnownHosts yes

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72253 - The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms. - RHEL-07-040400

Severity

Medium

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.

Fix

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "MACs" keyword and set its value to "hmac-sha2-256" and/or "hmac-sha2-512" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

MACs hmac-sha2-256,hmac-sha2-512

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon is configured to only use MACs employing FIPS 140-2-approved ciphers.

Note: If RHEL-07-021350 is a finding, this is automatically a finding as the system cannot implement FIPS 140-2-approved cryptographic algorithms and hashes.

Check that the SSH daemon is configured to only use MACs employing FIPS 140-2-approved ciphers with the following command:

grep -i macs /etc/ssh/sshd_config MACs hmac-sha2-256,hmac-sha2-512

If any ciphers other than "hmac-sha2-256" or "hmac-sha2-512" are listed or the retuned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001453

V-72255 - The SSH public host key files must have mode 0644 or less permissive. - RHEL-07-040410

Severity

Medium

Description

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Fix

Note: SSH public key files may be found in other directories on the system depending on the installation.

Change the mode of public host key files under "/etc/ssh" to "0644" with the following command:

chmod 0644 /etc/ssh/*.key.pub

Check

Verify the SSH public host key files have mode "0644" or less permissive.

Note: SSH public key files may be found in other directories on the system depending on the installation.

The following command will find all SSH public key files on the system:

find /etc/ssh -name '*.pub' -exec ls -lL {} ;

-rw-r–r– 1 root wheel 618 Nov 28 06:43 ssh_host_dsa_key.pub

-rw-r–r– 1 root wheel 347 Nov 28 06:43 ssh_host_key.pub

-rw-r–r– 1 root wheel 238 Nov 28 06:43 ssh_host_rsa_key.pub

If any file has a mode more permissive than "0644", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72257 - The SSH private host key files must have mode 0600 or less permissive. - RHEL-07-040420

Severity

Medium

Description

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Fix

Configure the mode of SSH private host key files under “/etc/ssh” to “0600” with the following command:

chmod 0600 /etc/ssh/ssh_host*key

Check

Verify the SSH private host key files have mode “0600” or less permissive.

The following command will find all SSH private key files on the system:

find / -name ‘*ssh_host*key’

Check the mode of the private host key files under “/etc/ssh” file with the following command:

ls -lL /etc/ssh/*key -rw——- 1 root wheel 668 Nov 28 06:43 ssh_host_dsa_key -rw——- 1 root wheel 582 Nov 28 06:43 ssh_host_key -rw——- 1 root wheel 887 Nov 28 06:43 ssh_host_rsa_key

If any file has a mode more permissive than “0600”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72259 - The SSH daemon must not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed. - RHEL-07-040430

Severity

Medium

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.

Fix

Uncomment the "GSSAPIAuthentication" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "no":

GSSAPIAuthentication no

The SSH service must be restarted for changes to take effect.

If GSSAPI authentication is required, it must be documented, to include the location of the configuration file, with the ISSO.

Check

Verify the SSH daemon does not permit GSSAPI authentication unless approved.

Check that the SSH daemon does not permit GSSAPI authentication with the following command:

grep -i gssapiauth /etc/ssh/sshd_config GSSAPIAuthentication no

If the "GSSAPIAuthentication" keyword is missing, is set to "yes" and is not documented with the Information System Security Officer (ISSO), or the returned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None

- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72261 - The SSH daemon must not permit Kerberos authentication unless needed. - RHEL-07-040440

Severity

Medium

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.

Fix

Uncomment the "KerberosAuthentication" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "no":

KerberosAuthentication no

The SSH service must be restarted for changes to take effect.

If Kerberos authentication is required, it must be documented, to include the location of the configuration file, with the ISSO.

Check

Verify the SSH daemon does not permit Kerberos to authenticate passwords unless approved.

Check that the SSH daemon does not permit Kerberos to authenticate passwords with the following command:

grep -i kerberosauth /etc/ssh/sshd_config KerberosAuthentication no

If the "KerberosAuthentication" keyword is missing, or is set to "yes" and is not documented with the Information System Security Officer (ISSO), or the returned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None

- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000318, CCI-000368, CCI-001812, CCI-001813, CCI-001814

V-72263 - The SSH daemon must perform strict mode checking of home directory configuration files. - RHEL-07-040450

Severity

Medium

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.

Fix

Uncomment the "StrictModes" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "yes":

StrictModes yes

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon performs strict mode checking of home directory configuration files.

The location of the "sshd_config" file may vary if a different daemon is in use.

Inspect the "sshd_config" file with the following command:

grep -i strictmodes /etc/ssh/sshd_config

StrictModes yes

If "StrictModes" is set to "no", is missing, or the returned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72265 - The SSH daemon must use privilege separation. - RHEL-07-040460

Severity

Medium

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.

Fix

Uncomment the "UsePrivilegeSeparation" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "sandbox" or "yes":

UsePrivilegeSeparation sandbox

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon performs privilege separation.

Check that the SSH daemon performs privilege separation with the following command:

grep -i usepriv /etc/ssh/sshd_config

UsePrivilegeSeparation sandbox

If the "UsePrivilegeSeparation" keyword is set to "no", is missing, or the retuned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72267 - The SSH daemon must not allow compression or must only allow compression after successful authentication. - RHEL-07-040470

Severity

Medium

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.

Fix

Uncomment the "Compression" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) on the system and set the value to "delayed" or "no":

Compression no

The SSH service must be restarted for changes to take effect.

Check

Verify the SSH daemon performs compression after a user successfully authenticates.

Check that the SSH daemon performs compression after a user successfully authenticates with the following command:

grep -i compression /etc/ssh/sshd_config Compression delayed

If the "Compression" keyword is set to "yes", is missing, or the retuned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72269 - The 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). - RHEL-07-040500

Severity

Medium

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.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

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

Fix

Edit the “/etc/ntp.conf” file and add or update an entry to define “maxpoll” to “10” as follows:

maxpoll 10

If NTP was running and “maxpoll” was updated, the NTP service must be restarted:

systemctl restart ntpd

If NTP was not running, it must be started:

systemctl start ntpd

Check

Check to see if NTP is running in continuous mode.

ps -ef | grep ntp

If NTP is not running, this is a finding.

If the process is found, then check the "ntp.conf" file for the "maxpoll" option setting:

grep maxpoll /etc/ntp.conf

maxpoll 17

If the option is set to "17" or is not set, this is a finding.

If the file does not exist, check the "/etc/cron.daily" subdirectory for a crontab file controlling the execution of the "ntpdate" command.

grep –l ntpdate /etc/cron.daily

ls -al /etc/cron.* | grep aide ntp

If a crontab file does not exist in the "/etc/cron.daily" that executes the "ntpdate" file, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001891, CCI-002046

V-72271 - The 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. - RHEL-07-040510

Severity

Medium

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.

Fix

Create a direct firewall rule to protect against DoS attacks with the following command:

Note: The command is to add a rule to the public zone.

firewall-cmd –direct –add-rule ipv4 filter IN_public_allow 0 -p tcp -m limit –limit 25/minute –limit-burst 100 -j ACCEPT

Check

Verify the operating system protects against or limits the effects of DoS attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

Check the firewall configuration with the following command:

Note: The command is to query rules for the public zone.

firewall-cmd –direct –get-rule ipv4 filter IN_public_allow rule ipv4 filter IN_public_allow 0 -p tcp -m limit –limit 25/minute –limit-burst 100 -j ACCEPT

If a rule with both the limit and limit-burst arguments parameters does not exist, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002385

V-72273 - The operating system must enable an application firewall, if available. - RHEL-07-040520

Severity

Medium

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

Fix

Ensure the operating system's application firewall is enabled.

Install the "firewalld" package, if it is not on the system, with the following command:

yum install firewalld

Start the firewall via "systemctl" with the following command:

systemctl start firewalld

Check

Verify the operating system enabled an application firewall.

Check to see if "firewalld" is installed with the following command:

yum list installed firewalld firewalld-0.3.9-11.el7.noarch.rpm

If the "firewalld" package is not installed, ask the System Administrator if another firewall application (such as iptables) is installed.

If an application firewall is not installed, this is a finding.

Check to see if the firewall is loaded and active with the following command:

systemctl status firewalld firewalld.service - firewalld - dynamic firewall daemon

> Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled) Active: active (running) since Tue 2014-06-17 11:14:49 CEST; 5 days ago

If "firewalld" does not show a status of "loaded" and "active", this is a finding.

Check the state of the firewall:

firewall-cmd –state running

If "firewalld" does not show a state of "running", this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72283 - The system must not forward Internet Protocol version 4 (IPv4) source-routed packets. - RHEL-07-040610

Severity

Medium

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.

Fix

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.conf.all.accept_source_route = 0

Check

Verify the system does not accept IPv4 source-routed packets.

Check the value of the accept source route variable with the following command:

/sbin/sysctl -a | grep net.ipv4.conf.all.accept_source_route net.ipv4.conf.all.accept_source_route=0

If the returned line does not have a value of "0", a line is not returned, or the returned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72285 - The system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default. - RHEL-07-040620

Severity

Medium

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.

Fix

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.conf.default.accept_source_route = 0

Check

Verify the system does not accept IPv4 source-routed packets by default.

Check the value of the accept source route variable with the following command:

/sbin/sysctl -a | grep net.ipv4.conf.default.accept_source_route net.ipv4.conf.default.accept_source_route=0

If the returned line does not have a value of "0", a line is not returned, or the returned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72287 - The system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address. - RHEL-07-040630

Severity

Medium

Description

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Fix

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.icmp_echo_ignore_broadcasts=1

Check

Verify the system does not respond to IPv4 ICMP echoes sent to a broadcast address.

Check the value of the "icmp_echo_ignore_broadcasts" variable with the following command:

/sbin/sysctl -a | grep net.ipv4.icmp_echo_ignore_broadcasts net.ipv4.icmp_echo_ignore_broadcasts=1

If the returned line does not have a value of "1", a line is not returned, or the retuned line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72289 - The system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted. - RHEL-07-040640

Severity

Medium

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.

Fix

Set the system to not accept IPv4 ICMP redirect messages by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.conf.default.accept_redirects = 0

Check

Verify the system will not accept IPv4 ICMP redirect messages.

Check the value of the default "accept_redirects" variables with the following command:

/sbin/sysctl -a | grep 'net.ipv4.conf.default.accept_redirects' net.ipv4.conf.default.accept_redirects=0

If the returned line does not have a value of "0", or a line is not returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72291 - The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default. - RHEL-07-040650

Severity

Medium

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.

Fix

Configure the system to not allow interfaces to perform IPv4 ICMP redirects by default.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.conf.default.send_redirects=0

Check

Verify the system does not allow interfaces to perform IPv4 ICMP redirects by default.

Check the value of the "default send_redirects" variables with the following command:

grep 'net.ipv4.conf.default.send_redirects' /etc/sysctl.conf net.ipv4.conf.default.send_redirects=0

If the returned line does not have a value of "0", or a line is not returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72293 - The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects. - RHEL-07-040660

Severity

Medium

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.

Fix

Configure the system to not allow interfaces to perform IPv4 ICMP redirects.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.conf.all.send_redirects=0

Check

Verify the system does not send IPv4 ICMP redirect messages.

Check the value of the "all send_redirects" variables with the following command:

grep 'net.ipv4.conf.all.send_redirects' /etc/sysctl.conf

net.ipv4.conf.all.send_redirects=0

If the returned line does not have a value of "0", or a line is not returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72295 - Network interfaces must not be in promiscuous mode. - RHEL-07-040670

Severity

Medium

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 then 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.

Fix

Configure network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.

Set the promiscuous mode of an interface to off with the following command:

#ip link set dev <devicename> multicast off promisc off

Check

Verify network interfaces are not in promiscuous mode unless approved by the ISSO and documented.

Check for the status with the following command:

ip link | grep -i promisc

If network interfaces are found on the system in promiscuous mode and their use has not been approved by the ISSO and documented, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72297 - The system must be configured to prevent unrestricted mail relaying. - RHEL-07-040680

Severity

Medium

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.

Fix

If “postfix” is installed, modify the “/etc/postfix/main.cf” file to restrict client connections to the local network with the following command:

postconf -e ‘smtpd_client_restrictions = permit_mynetworks,reject’

Check

Verify the system is configured to prevent unrestricted mail relaying.

Determine if “postfix” is installed with the following commands:

yum list installed postfix postfix-2.6.6-6.el7.x86_64.rpm

If postfix is not installed, this is Not Applicable.

If postfix is installed, determine if it is configured to reject connections from unknown or untrusted networks with the following command:

postconf -n smtpd_client_restrictions smtpd_client_restrictions = permit_mynetworks, reject

If the “smtpd_client_restrictions” parameter contains any entries other than “permit_mynetworks” and “reject”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72305 - If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode. - RHEL-07-040720

Severity

Medium

Description

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Fix

Configure the TFTP daemon to operate in secure mode by adding the following line to “/etc/xinetd.d/tftp” (or modify the line to have the required value):

server_args = -s /var/lib/tftpboot

Check

Verify the TFTP daemon is configured to operate in secure mode.

Check to see if a TFTP server has been installed with the following commands:

yum list installed | grep tftp tftp-0.49-9.el7.x86_64.rpm

If a TFTP server is not installed, this is Not Applicable.

If a TFTP server is installed, check for the server arguments with the following command:

grep server_arge /etc/xinetd.d/tftp server_args = -s /var/lib/tftpboot

If the "server_args" line does not have a "-s" option and a subdirectory is not assigned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72307 - An X Windows display manager must not be installed unless approved. - RHEL-07-040730

Severity

Medium

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.

Fix

Document the requirement for an X Windows server with the ISSO or remove the related packages with the following commands:

#yum groupremove "X Window System"

#yum remove xorg-x11-server-common

Check

Verify that if the system has X Windows System installed, it is authorized.

Check for the X11 package with the following command:

yum group list installed “X Window System”

Ask the System Administrator if use of the X Windows System is an operational requirement.

If the use of X Windows on the system is not documented with the Information System Security Officer (ISSO), this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72309 - The system must not be performing packet forwarding unless the system is a router. - RHEL-07-040740

Severity

Medium

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.

Fix

Set the system to the required kernel parameter by adding the following line to “/etc/sysctl.conf” (or modify the line to have the required value):

net.ipv4.ip_forward = 0

Check

Verify the system is not performing packet forwarding, unless the system is a router.

Check to see if IP forwarding is enabled using the following command:

/sbin/sysctl -a | grep net.ipv4.ip_forward net.ipv4.ip_forward=0

If IP forwarding value is “1” and the system is hosting any application, database, or web servers, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72311 - The Network File System (NFS) must be configured to use RPCSEC_GSS. - RHEL-07-040750

Severity

Medium

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.

Fix

Update the “/etc/fstab” file so the option “sec” is defined for each NFS mounted file system and the “sec” option does not have the “sys” setting.

Ensure the “sec” option is defined as “krb5:krb5i:krb5p”.

Check

Verify "AUTH_GSS" is being used to authenticate NFS mounts.

To check if the system is importing an NFS file system, look for any entries in the "/etc/fstab" file that have a file system type of "nfs" with the following command:

cat /etc/fstab | grep nfs 192.168.21.5:/mnt/export /data1 nfs4 rw,sync ,soft,sec=krb5:krb5i:krb5p

If the system is mounting file systems via NFS and has the sec option without the "krb5:krb5i:krb5p" settings, the "sec" option has the "sys" setting, or the "sec" option is missing, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72315 - The system access control program must be configured to grant or deny system access to specific hosts and services. - RHEL-07-040810

Severity

Medium

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.

Fix

If "firewalld" is installed and active on the system, configure rules for allowing specific services and hosts.

If "tcpwrappers" is installed, configure the "/etc/hosts.allow" and "/etc/hosts.deny" to allow or deny access to specific hosts.

Check

If the “firewalld” package is not installed, ask the System Administrator (SA) if another firewall application (such as iptables) is installed. If an application firewall is not installed, this is a finding.

Verify the system’s access control program is configured to grant or deny system access to specific hosts.

Check to see if “firewalld” is active with the following command:

systemctl status firewalld firewalld.service - firewalld - dynamic firewall daemon

> Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled) Active: active (running) since Sun 2014-04-20 14:06:46 BST; 30s ago

If “firewalld” is active, check to see if it is configured to grant or deny access to specific hosts or services with the following commands:

firewall-cmd –get-default-zone public

firewall-cmd –list-all –zone=public public (default, active)

> interfaces: eth0 sources: services: mdns ssh ports: masquerade: no forward-ports: icmp-blocks: rich rules:
>
> rule family=”ipv4” source address=”92.188.21.1/24” accept rule family=”ipv4” source address=”211.17.142.46/32” accept

If “firewalld” is not active, determine whether “tcpwrappers” is being used by checking whether the “hosts.allow” and “hosts.deny” files are empty with the following commands:

ls -al /etc/hosts.allow rw-r—– 1 root root 9 Aug 2 23:13 /etc/hosts.allow

ls -al /etc/hosts.deny -rw-r—– 1 root root 9 Apr 9 2007 /etc/hosts.deny

If “firewalld” and “tcpwrappers” are not installed, configured, and active, ask the SA if another access control program (such as iptables) is installed and active. Ask the SA to show that the running configuration grants or denies access to specific hosts or services.

If “firewalld” is active and is not configured to grant access to specific hosts and “tcpwrappers” is not configured to grant or deny access to specific hosts, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72317 - The system must not have unauthorized IP tunnels configured. - RHEL-07-040820

Severity

Medium

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).

Fix

Remove all unapproved tunnels from the system, or document them with the ISSO.

Check

Verify the system does not have unauthorized IP tunnels configured.

Check to see if “libreswan” is installed with the following command:

yum list installed libreswan openswan-2.6.32-27.el6.x86_64

If “libreswan” is installed, check to see if the “IPsec” service is active with the following command:

systemctl status ipsec ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec

Loaded: loaded (/usr/lib/systemd/system/ipsec.service; disabled) Active: inactive (dead)

If the “IPsec” service is active, check to see if any tunnels are configured in “/etc/ipsec.conf” and “/etc/ipsec.d/” with the following commands:

grep -i conn /etc/ipsec.conf conn mytunnel

grep -i conn /etc/ipsec.d/*.conf conn mytunnel

If there are indications that a “conn” parameter is configured for a tunnel, ask the System Administrator if the tunnel is documented with the ISSO. If “libreswan” is installed, “IPsec” is active, and an undocumented tunnel is active, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None

- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72319 - The system must not forward IPv6 source-routed packets. - RHEL-07-040830

Severity

Medium

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.

Fix

Set the system to the required kernel parameter, if IPv6 is enabled, by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv6.conf.all.accept_source_route = 0

Check

Verify the system does not accept IPv6 source-routed packets.

Note: If IPv6 is not enabled, the key will not exist, and this is not a finding.

Check the value of the accept source route variable with the following command:

/sbin/sysctl -a | grep net.ipv6.conf.all.accept_source_route net.ipv6.conf.all.accept_source_route=0

If the returned lines do not have a value of "0", or a line is not returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72417 - The operating system must have the required packages for multifactor authentication installed. - RHEL-07-041001

Severity

Medium

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

Fix

Configure the operating system to implement multifactor authentication by installing the required packages.

Install the “esc”, “pam_pkcs11”, “authconfig”, and “authconfig-gtk” packages on the system with the following command:

yum install esc pam_pkcs11 authconfig-gtk

Check

Verify the operating system has the packages required for multifactor authentication installed.

Check for the presence of the packages required to support multifactor authentication with the following commands:

yum list installed esc esc-1.1.0-26.el7.noarch.rpm

yum list installed pam_pkcs11 pam_pkcs11-0.6.2-14.el7.noarch.rpm

yum list installed authconfig-gtk authconfig-gtk-6.1.12-19.el7.noarch.rpm

If the “esc”, “pam_pkcs11”, and “authconfig-gtk” packages are not installed, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001948, CCI-001953, CCI-001954

V-72427 - The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM). - RHEL-07-041002

Severity

Medium

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

Fix

Configure the operating system to implement multifactor authentication for remote access to privileged accounts via pluggable authentication modules (PAM).

Modify all of the services lines in /etc/sssd/sssd.conf to include pam.

Check

Verify the operating system implements multifactor authentication for remote access to privileged accounts via pluggable authentication modules (PAM).

Check the "/etc/sssd/sssd.conf" file for the authentication services that are being used with the following command:

grep services /etc/sssd/sssd.conf

services = nss, pam

If the "pam" service is not present, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001948, CCI-001953, CCI-001954

V-72433 - The operating system must implement certificate status checking for PKI authentication. - RHEL-07-041003

Severity

Medium

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

Fix

Configure the operating system to do certificate status checking for PKI authentication.

Modify all of the “cert_policy” lines in “/etc/pam_pkcs11/pam_pkcs11.conf” to include “ocsp_on”.

Check

Verify the operating system implements certificate status checking for PKI authentication.

Check to see if Online Certificate Status Protocol (OCSP) is enabled on the system with the following command:

grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf

cert_policy =ca, ocsp_on, signature; cert_policy =ca, ocsp_on, signature; cert_policy =ca, ocsp_on, signature;

There should be at least three lines returned. All lines must match the example output; specifically that “oscp_on” must be included in the “cert_policy” line.

If “oscp_on” is present in all “cert_policy” lines, this is not a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None

- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001948, CCI-001953, CCI-001954

V-72435 - The operating system must implement smart card logons for multifactor authentication for access to privileged accounts. - RHEL-07-041004

Severity

Medium

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

Fix

Configure the operating system to implement smart card logon for multifactor authentication to uniquely identify privileged users.

Enable smart card logons with the following commands:

#authconfig –enablesmartcard –smartcardaction=1 –update # authconfig –enablerequiresmartcard –update

Check

Verify the operating system requires smart card logons for multifactor authentication to uniquely identify privileged users.

Check to see if smartcard authentication is enforced on the system with the following command:

authconfig –test | grep -i smartcard

The entry for use only smartcard for logon may be enabled, and the smartcard module and smartcard removal actions must not be blank.

If smartcard authentication is disabled or the smartcard and smartcard removal actions are blank, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001948, CCI-001953, CCI-001954

V-73155 - The operating system must set the lock delay setting for all connection types. - RHEL-07-010081

Severity

Medium

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.

Fix

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

touch /etc/dconf/db/local.d/locks/session

Add the setting to lock the screensaver lock delay:

/org/gnome/desktop/screensaver/lock-delay

Check

Verify the operating system prevents a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.

Determine which profile the system database is using with the following command: # grep system-db /etc/dconf/profile/user

system-db:local

Check for the lock delay setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

grep -i lock-delay /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/lock-delay

If the command does not return a result, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-73157 - The operating system must set the session idle delay setting for all connection types. - RHEL-07-010082

Severity

Medium

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.

Fix

Configure the operating system to prevent a user from overriding a session lock after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in /etc/dconf/profile/user, the file should be created under the appropriate subdirectory.

touch /etc/dconf/db/local.d/locks/session

Add the setting to lock the session idle delay:

/org/gnome/desktop/session/idle-delay

Check

Verify the operating system prevents a user from overriding session idle delay after a 15-minute period of inactivity for graphical user interfaces. The screen program must be installed to lock sessions on the console.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command: # grep system-db /etc/dconf/profile/user

system-db:local

Check for the session idle delay setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

grep -i idle-delay /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/session/idle-delay

If the command does not return a result, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000057

V-73159 - When passwords are changed or new passwords are established, pwquality must be used. - RHEL-07-010119

Severity

Medium

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 on the system.

Fix

Configure the operating system to use “pwquality” to enforce password complexity rules.

Add the following line to “/etc/pam.d/passwd” (or modify the line to have the required value):

password required pam_pwquality.so retry=3

Check

Verify the operating system uses “pwquality” to enforce the password complexity rules.

Check for the use of “pwquality” with the following command:

grep pwquality /etc/pam.d/passwd

password required pam_pwquality.so retry=3

If the command does not return a line containing the value “pam_pwquality.so”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000192

V-73161 - File systems that are being imported via Network File System (NFS) must be mounted to prevent binary files from being executed. - RHEL-07-021021

Severity

Medium

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.

Fix

Configure the "/etc/fstab" to use the "noexec" option on file systems that are being exported via NFS.

Check

Verify file systems that are being NFS exported are mounted with the "noexec" option.

Find the file system(s) that contain the directories being exported with the following command:

more /etc/fstab | grep nfs

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,noexec 0 0

If a file system found in "/etc/fstab" refers to NFS and it does not have the "noexec" option set, and use of NFS exported binaries is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-73163 - The audit system must take appropriate action when there is an error sending audit records to a remote system. - RHEL-07-030321

Severity

Medium

Description

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

Fix

Configure the action the operating system takes if there is an error sending audit records to a remote system.

Uncomment the “network_failure_action” option in “/etc/audisp/audisp-remote.conf” and set it to “syslog”, “single”, or “halt”.

network_failure_action = single

Check

Verify the action the operating system takes if there is an error sending audit records to a remote system.

Check the action that takes place if there is an error sending audit records to a remote system with the following command:

grep -i network_failure_action /etc/audisp/audisp-remote.conf network_failure_action = stop

If the value of the “network_failure_action” option is not “syslog”, “single”, or “halt”, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None

- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001851

V-73165 - The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group. - RHEL-07-030871

Severity

Medium

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).

Fix

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-w /etc/group -p wa -k identity

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep /etc/group /etc/audit/audit.rules

-w /etc/group -p wa -k audit_rules_usergroup_modification

If the command does not return a line, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000018, CCI-000172, CCI-001403, CCI-002130

V-73167 - The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow. - RHEL-07-030872

Severity

Medium

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).

Fix

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-w /etc/gshadow -p wa -k identity

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep /etc/gshadow /etc/audit/audit.rules

-w /etc/gshadow -p wa -k audit_rules_usergroup_modification

If the command does not return a line, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000018, CCI-000172, CCI-001403, CCI-002130

V-73171 - The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow. - RHEL-07-030873

Severity

Medium

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).

Fix

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Add or update the following file system rule in "/etc/audit/rules.d/audit.rules":

-w /etc/shadow -p wa -k identity

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

grep /etc/shadow /etc/audit/audit.rules

-w /etc/shadow -p wa -k audit_rules_usergroup_modification

If the command does not return a line, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000018, CCI-000172, CCI-001403, CCI-002130

V-73173 - The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd. - RHEL-07-030874

Severity

Medium

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).

Fix

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

Add or update the following file system rule in "/etc/audit/rules.d/audit.rules":

-w /etc/opasswd -p wa -k identity

The audit daemon must be restarted for the changes to take effect.

Check

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

Check the auditing rules in "/etc/audit/rules.d/audit.rules" with the following command:

grep /etc/opasswd /etc/audit/rules.d/audit.rules

-w /etc/opasswd -p wa -k audit_rules_usergroup_modification

If the command does not return a line, or the line is commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000018, CCI-000172, CCI-001403, CCI-002130

V-73175 - The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages. - RHEL-07-040641

Severity

Medium

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.

Fix

Set the system to ignore IPv4 ICMP redirect messages by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

net.ipv4.conf.all.accept_redirects = 0

Check

Verify the system ignores IPv4 ICMP redirect messages.

Check the value of the "accept_redirects" variables with the following command:

/sbin/sysctl -a | grep 'net.ipv4.conf.all.accept_redirects'

net.ipv4.conf.all.accept_redirects=0

If both of the returned lines do not have a value of "0", or a line is not returned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-73177 - Wireless network adapters must be disabled. - RHEL-07-041010

Severity

Medium

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.

Fix

Configure the system to disable all wireless network interfaces with the following command:

#nmcli radio wifi off

Check

Verify that there are no wireless interfaces configured on the system.

This is N/A for systems that do not have wireless network adapters.

Check for the presence of active wireless interfaces with the following command:

nmcli device DEVICE TYPE STATE eth0 ethernet connected wlp3s0 wifi disconnected lo loopback unmanaged

If a wireless interface is configured and its use on the system is not documented with the Information System Security Officer (ISSO), this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-001443, CCI-001444, CCI-002418

CHAPTER 3

Cat III (Low Severity)

Low

V-71987 - The operating system must remove all software components after updated versions have been installed. - RHEL-07-020200

Severity

Low

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.

Fix

Configure the operating system to remove all software components after updated versions have been installed.

Set the “clean_requirements_on_remove” option to “1” in the “/etc/yum.conf” file:

clean_requirements_on_remove=1

Check

Verify the operating system removes all software components after updated versions have been installed.

Check if yum is configured to remove unneeded packages with the following command:

grep -i clean_requirements_on_remove /etc/yum.conf clean_requirements_on_remove=1

If “clean_requirements_on_remove” is not set to “1”, “True”, or “yes”, or is not set in “/etc/yum.conf”, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-002617

V-72003 - All Group Identifiers (GIDs) referenced in the /etc/passwd file must be defined in the /etc/group file. - RHEL-07-020300

Severity

Low

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.

Fix

Configure the system to define all GIDs found in the “/etc/passwd” file by modifying the “/etc/group” file to add any non-existent group referenced in the “/etc/passwd” file, or change the GIDs referenced in the “/etc/passwd” file to a group that exists in “/etc/group”.

Check

Verify all GIDs referenced in the “/etc/passwd” file are defined in the “/etc/group” file.

Check that all referenced GIDs exist with the following command:

pwck -r

If GIDs referenced in “/etc/passwd” file are returned as not defined in “/etc/group” file, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000764

V-72059 - A separate file system must be used for user home directories (such as /home or an equivalent). - RHEL-07-021310

Severity

Low

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.

Fix

Migrate the "/home" directory onto a separate file system/partition.

Check

Verify that a separate file system/partition has been created for non-privileged local interactive user home directories.

Check the home directory assignment for all non-privileged users (those with a UID greater than 1000) on the system with the following command:

#cut -d: -f 1,3,6,7 /etc/passwd | egrep ":[1-4][0-9]{3}" | tr ":" "t"

adamsj /home/adamsj /bin/bash jacksonm /home/jacksonm /bin/bash smithj /home/smithj /bin/bash

The output of the command will give the directory/partition that contains the home directories for the non-privileged users on the system (in this example, /home) and users' shell. All accounts with a valid shell (such as /bin/bash) are considered interactive users.

Check that a file system/partition has been created for the non-privileged interactive users with the following command:

Note: The partition of /home is used in the example.

grep /home /etc/fstab UUID=333ada18 /home ext4 noatime,nobarrier,nodev 1 2

If a separate entry for the file system/partition that contains the non-privileged interactive users' home directories does not exist, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72061 - The system must use a separate file system for /var. - RHEL-07-021320

Severity

Low

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.

Fix

Migrate the "/var" path onto a separate file system.

Check

Verify that a separate file system/partition has been created for "/var".

Check that a file system/partition has been created for "/var" with the following command:

grep /var /etc/fstab UUID=c274f65f /var ext4 noatime,nobarrier 1 2

If a separate entry for "/var" is not in use, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72063 - The system must use a separate file system for the system audit data path. - RHEL-07-021330

Severity

Low

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.

Fix

Migrate the system audit data path onto a separate file system.

Check

Verify the file integrity tool is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Note: If RHEL-07-021350 is a finding, this is automatically a finding as the system cannot implement FIPS 140-2 approved cryptographic algorithms and hashes.

Check to see if Advanced Intrusion Detection Environment (AIDE) is installed on the system with the following command:

yum list installed aide

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

If there is no application installed to perform file integrity checks, this is a finding.

Note: AIDE is highly configurable at install time. These commands assume the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

find / -name aide.conf

Check the "aide.conf" file to determine if the "sha512" rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the "sha512" rule follows:

All=p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux /bin All # apply the custom rule to the files in bin /sbin All # apply the same custom rule to the files in sbin

If the "sha512" rule is not being used on all selection lines in the "/etc/aide.conf" file, or another file integrity tool is not using FIPS 140-2 approved cryptographic hashes for validating file contents and directories, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72065 - The system must use a separate file system for /tmp (or equivalent). - RHEL-07-021340

Severity

Low

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.

Fix

Start the “tmp.mount” service with the following command:

systemctl enable tmp.mount

Check

Verify that a separate file system/partition has been created for “/tmp”.

Check that a file system/partition has been created for “/tmp” with the following command:

systemctl is-enabled tmp.mount enabled

If the “tmp.mount” service is not enabled, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72069 - The file integrity tool must be configured to verify Access Control Lists (ACLs). - RHEL-07-021600

Severity

Low

Description

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

Fix

Configure the file integrity tool to check file and directory ACLs.

If AIDE is installed, ensure the “acl” rule is present on all file and directory selection lists.

Check

Verify the file integrity tool is configured to verify ACLs.

Check to see if Advanced Intrusion Detection Environment (AIDE) is installed on the system with the following command:

yum list installed aide

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

If there is no application installed to perform file integrity checks, this is a finding.

Note: AIDE is highly configurable at install time. These commands assume the “aide.conf” file is under the “/etc” directory.

Use the following command to determine if the file is in another location:

find / -name aide.conf

Check the “aide.conf” file to determine if the “acl” rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the “acl” rule is below:

All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux /bin All # apply the custom rule to the files in bin /sbin All # apply the same custom rule to the files in sbin

If the “acl” rule is not being used on all selection lines in the “/etc/aide.conf” file, or ACLs are not being checked by another file integrity tool, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72071 - The file integrity tool must be configured to verify extended attributes. - RHEL-07-021610

Severity

Low

Description

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

Fix

Configure the file integrity tool to check file and directory extended attributes.

If AIDE is installed, ensure the “xattrs” rule is present on all file and directory selection lists.

Check

Verify the file integrity tool is configured to verify extended attributes.

Check to see if Advanced Intrusion Detection Environment (AIDE) is installed on the system with the following command:

yum list installed aide

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

If there is no application installed to perform file integrity checks, this is a finding.

Note: AIDE is highly configurable at install time. These commands assume the “aide.conf” file is under the “/etc” directory.

Use the following command to determine if the file is in another location:

find / -name aide.conf

Check the “aide.conf” file to determine if the “xattrs” rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the “xattrs” rule follows:

All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux /bin All # apply the custom rule to the files in bin /sbin All # apply the same custom rule to the files in sbin

If the “xattrs” rule is not being used on all selection lines in the “/etc/aide.conf” file, or extended attributes are not being checked by another file integrity tool, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None

- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72217 - The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types. - RHEL-07-040000

Severity

Low

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.

Fix

Configure the operating system to limit the number of concurrent sessions to “10” for all accounts and/or account types.

Add the following line to the top of the /etc/security/limits.conf:

- hard maxlogins 10

Check

Verify the operating system limits the number of concurrent sessions to “10” for all accounts and/or account types by issuing the following command:

grep “maxlogins” /etc/security/limits.conf * hard maxlogins 10

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.

If the “maxlogins” item is missing or the value is not set to “10” or less for all domains that have the “maxlogins” item assigned, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000054

V-72275 - The system must display the date and time of the last successful account logon upon logon. - RHEL-07-040530

Severity

Low

Description

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Fix

Configure the operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin-ac".

Add the following line to the top of "/etc/pam.d/postlogin-ac":

session required pam_lastlog.so showfailed

Check

Verify users are provided with feedback on when account accesses last occurred.

Check that "pam_lastlog" is used and not silent with the following command:

grep pam_lastlog /etc/pam.d/postlogin-ac

session required pam_lastlog.so showfailed silent

If "pam_lastlog" is missing from "/etc/pam.d/postlogin-ac" file, or the silent option is present on the line check for the "PrintLastLog" keyword in the sshd daemon configuration file, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366

V-72281 - For systems using DNS resolution, at least two name servers must be configured. - RHEL-07-040600

Severity

Low

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.

Fix

Configure the operating system to use two or more name servers for DNS resolution.

Edit the "/etc/resolv.conf" file to uncomment or add the two or more "nameserver" option lines with the IP address of local authoritative name servers. If local host resolution is being performed, the "/etc/resolv.conf" file must be empty. An empty "/etc/resolv.conf" file can be created as follows:

echo -n > /etc/resolv.conf

And then make the file immutable with the following command:

chattr +i /etc/resolv.conf

If the "/etc/resolv.conf" file must be mutable, the required configuration must be documented with the Information System Security Officer (ISSO) and the file must be verified by the system file integrity tool.

Check

Determine whether the system is using local or DNS name resolution with the following command:

grep hosts /etc/nsswitch.conf hosts: files dns

If the DNS entry is missing from the host's line in the "/etc/nsswitch.conf" file, the "/etc/resolv.conf" file must be empty.

Verify the "/etc/resolv.conf" file is empty with the following command:

ls -al /etc/resolv.conf -rw-r–r– 1 root root 0 Aug 19 08:31 resolv.conf

If local host authentication is being used and the "/etc/resolv.conf" file is not empty, this is a finding.

If the DNS entry is found on the host's line of the "/etc/nsswitch.conf" file, verify the operating system is configured to use two or more name servers for DNS resolution.

Determine the name servers used by the system with the following command:

grep nameserver /etc/resolv.conf nameserver 192.168.1.2 nameserver 192.168.1.3

If less than two lines are returned that are not commented out, this is a finding.

Additional Data

- Documentable: false
- False Negatives: None
- False Positives: None
- IA Controls: None
- Mitigation Control: None
- Mitigations: None
- Potential Impacts: None
- Responsibility: None
- SeverityOverrideGuidance: None
- Third Party Tools: None
- Control Correlation Identifiers: CCI-000366