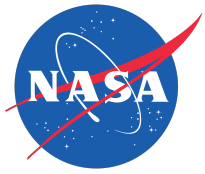

NASA TECHNICAL SPECIFICATION

National Aeronautics and Space Administration

NASA-SPEC-2601OS.RHEL8 v1.7
Approved: 2023-06-05

Superseding: NASA-SPEC-2601OS.RHEL8 v1.6

RED HAT ENTERPRISE LINUX 8
SECURITY CONFIGURATION SPECIFICATION

TABLE OF CONTENTS

Document History Log

Document Version	Date Approved	Description
1.7	2023-06-05	Release 4 FY2023
1.6	2023-01-30	Release 2 FY2023
1.5	2022-07-25	updated for SUN spec
1.4	2021-11-05	Added PIV and DAR checks
1.2	2021-02-11	Release 1 2021
1.1	2020-08-26	Additions with DEFEND Aware alignment.
1.0	2020-02-20	Initial Release

Foreword

This NASA Technical Specification is published by the National Aeronautics and Space Administration (NASA) to describe technical requirements for purchased or in-house items, services, functions, or processes for NASA programs and projects.

This NASA Technical Specification is approved for use by NASA Headquarters and NASA Centers and Facilities, and applicable technical requirements may be cited in contract, program, and other NASA documents. This Specification also applies to the Jet Propulsion Laboratory (JPL) (a Federally Funded Research and Development Center (FFRDC)), other contractors, recipients of grants and cooperative agreements, and parties to other agreements only to the extent specified or referenced in applicable contracts, grants, or agreements.

Adherence to this NASA Technical Specification ensures compliance with NASA-STD-2601, *Minimum Cybersecurity Requirements for Computing Systems*, which defines operating system and application security requirements that must be implemented on NASA information systems. This Specification provides the enforceable, measurable details of NASA-STD-2601.

Comments, concerns, and all other feedback on this Specification can be submitted via email to NASA-DL-ASCS-TECHNICAL@mail.nasa.gov.

Refer to NASA-SPEC-2600, *Enumeration of ASCS Cybersecurity Requirements* for signature.

1. Scope

1.1. Purpose

The purpose of this NASA Technical Specification is to define version and configuration requirements for Red Hat Enterprise Linux 8 deployment and operation.

1.2. Applicability

This NASA Technical Specification is applicable to all computing systems using Red Hat Enterprise Linux 8.

This NASA Technical Specification is approved for use by NASA Headquarters and NASA Centers and Facilities, and applicable technical requirements may be cited in contract, program, and other NASA documents. This Specification also applies to JPL, other contractors, recipients of grants and cooperative agreements, and parties to other agreements only to the extent specified or referenced in applicable contracts, grants, or agreements.

1.3. Tailoring

Each security configuration setting defined in this NASA Technical Specification is assigned an ASCS severity rating of *Critical*, *High*, *Medium*, or *Low*. The process for deviating from security configuration settings varies based on each setting's ASCS severity rating.

Each security configuration setting protects against the exploitation of a vulnerability, and ASCS severity ratings are assigned to settings based on the potential impact that a system would incur if the associated vulnerability were exploited. This is why the process for deviating from settings is based on severity rating.

***Critical* and *High* Severity Ratings:**

Security configuration settings with *Critical* or *High* severity ratings ***SHALL NOT*** be tailored out of the System Security Plan (SSP). If a specific program, project, or system is unable to fully implement a setting with a *Critical* or *High* severity rating, a Plan of Action and Milestones (POA&Ms) or risk-based decision (RBD) addressing this need ***SHALL*** be approved by the NASA Chief Information Officer (CIO) or designee, and the RBD ***SHALL*** be formally documented in the system's SSP under program or project requirements.

***Medium* Severity Rating:**

If a specific program, project, or system is unable to fully implement a setting with a *Medium* severity rating a POA&M or RBD addressing this need ***SHALL*** be approved by the responsible Information System Owner (ISO) and the Authorizing Official (AO) (or Authorizing Official Designated Representative (AODR), if applicable) and formally documented by the ISO or system administrator(s) in the SSP under program or project requirements. The AO ***SHALL*** ensure that only systems posing an acceptable level of risk (LOR) to NASA assets, data, and personnel are approved for production operation and that all necessary documentation is produced and maintained.

***Low* Severity Rating:**

Security configuration settings with a *Low* severity rating are expected to be implemented unless there is a justifiable cause not to. Deviations from security configuration settings with a Low severity rating will not impact a system's compliance score.

1.4. Authority

The NASA Chief Information Officer (CIO) and Senior Agency Information Security Officer (SAISO) have authorized the Cybersecurity Standards and Engineering Team (CSET) via the Agency Security Configuration Standards (ASCS) initiative to create binding Technical Standards related to cybersecurity topics.

The NASA Technical Standards Program (NTSP), sponsored by the Office of the NASA Chief Engineer, recognizes CSET as a standards-developing organization within NASA.

In accordance with NPR 2810.1F, *Security of Information and Information Systems*, ISOs ***SHALL*** implement the requirements and settings defined in all applicable standards and specifications established by ASCS.

2. Applicable Documents

2.1. Government Documents

Table 1. NASA Documents

Document Identifier	Document Title
NASA-STD-2601	*Minimum Cybersecurity Requirements for Computing Systems*
NPR 2810.1*x*	*Security of Information Technology*

Table 2. Other Government Documents

Document Number or Descriptor	Document Title
FIPS 140-2 Validated Modules	*Federal Information Processing Standards Validation Program*
NASA-HDBK-2602	*NASA Data At Rest Handbook*
DISA STIG	*Red Hat Enterprise Linux 8 STIG - Ver 1, Rel 7*
NASA-STD-2601	*Minimum Cybersecurity Requirements for Computing Systems*
NPR 2810.1	*Security of Information Technology*

2.2. Non-Government Documents

Document Number or Descriptor	Document Title
Center for Internet Security	*CIS Red Hat Enterprise Linux 8 Benchmark v2.0.0*

3. Acronyms, Abbreviations, and Definitions

Table 3. Acronyms and Abbreviations

NASA	National Aeronautics and Space Administration
ACL (Security)	Access Control List
ACL (Procurement)	Assessed and Cleared List
AO	Authorizing Official
ASCS	Agency Security Configuration Standards
ASRL	Address Space Layout Randomization
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIS	Center for Internet Security
CSET	Cybersecurity Standards and Engineering Team
CUPS	Common Unix Printing System
DAC	Directory Access Controls
DCCP	Datagram Congestion Control Protocol
DAR	Data At Rest
DHCP	Dynamic Host Configuration Protocol
DISA	Defence Information System Agency
ESD	Enterprise Service Desk
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FPKI	Federal Public Key Infrastructure
ICAM	Identity, Credential, and Access Management
ICMP	Internet Control Message Protocol
IDI	ICAM Device Integration
idM	Identity Management (Red Hat Product)
ISO	Information System Owner
JPL	Jet Propulsion Laboratory
LVM	Logical Volume Manager
LUKS	Linux Unified Key Setup
MAC (Security)	Mandatory Access Control
MAC (Network)	Media Access Control
NCTR	NASA Client Trust Reference

NASA	National Aeronautics and Space Administration
NFS	Network File System
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirement
NSA	National Security Agency
NTAM	NASA Trust Anchor Management
NTSP	NASA Technical Standards Panel
OCIO	Office of the Chief Information Officer
PKI	Public Key Infrastructure
RISCS	Risk Information and Security Compliance System
ROP	Return Oriented Programming
SAISO	Senior Agency Information Security Officer
SCAP	Security Content Automation Protocol
SCTP	Stream Control Transmission Protocol
SGID	Set Group ID
SOC	Security Operations Center
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SUID	Set User ID
TFTP	Trivial File Transfer Protocol
XCCDF	eXtensible Configuration Checklist Description Format

4. Version and Lifecycle

This Specification applies to the Operating System defined in the chart below, as well as to any more recent version(s) of this Operating System.

Function	Operating System
Application	Red Hat Enterprise Linux 8
Minimum Version	Vendor supplied latest version built to meet FIPS validation

5. Security Configurations

5.1. Critical Severity Settings

Critical severity settings ***SHALL*** be adhered to, as they are monitored, scored, and reported to the Department of Homeland Security (DHS).

- *Critical* severity settings target any vulnerability which, if exploited, would directly and immediately result in the loss of confidentiality, integrity, or availability.
- *Critical* severity settings are reported by the Continuous Diagnosis and Mitigation (CDM) Defend Dashboard and/or mandated by Federal policy.
- Deviations from *critical* severity settings require approval from the NASA CIO or CIO designee.

NASA-ASCS-20014: Require Authentication for Single User Mode

NASA ASCS ID	NASA-ASCS-20014
Severity	**Critical**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-010151, RHEL_8_STIG RHEL-08-010140, RHEL_8_STIG RHEL-08-010150

Single-user mode is intended as a system recovery method, providing a single user root access to the system by providing a boot option at startup. Use of `sulogin`, which comes in different forms on different platforms, will show up in some form in the rescue control configuration. Systems set to `sushell` will need to be configured properly.

On `systemd`, single-user mode is protected by requiring a use of a `sulogin` set in `rescue.service`, this can be viewed with the `systemctl` command.

```
systemctl cat rescue.service | grep "^ExecStart="
```

On `SysV`, single-user mode is protected by requiring a password when `/etc/sysconfig/init` contains the line `SINGL=/sbin/sulogin`

Rationale

This prevents attackers with physical access from trivially bypassing security on the machine and gaining root access. Such accesses are further prevented by configuring the bootloader password.

bash fix

```
if ! systemctl cat rescue.service | grep -q "^ExecStart=\-.*sulogin" &> /dev/null
then
  RESCUE_SERVICE_FILE=$( find /usr/lib{,64} -name rescue.service )
  sed -i "s/^ExecStart=.*/ExecStart=\-\/usr\/lib\/systemd\/systemd\-sulogin\-shell\ rescue/"
$RESCUE_SERVICE_FILE
fi
```

NASA-ASCS-20121: Verify Only Root Has UID 0

NASA ASCS ID	NASA-ASCS-20121
Severity	**Critical**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-040200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.8
MITRE ATT&CK Reference	TA0004, M1026

If any account other than root has a UID of 0, this misconfiguration shall be investigated. Accounts other than root shall be removed or have their UID changed.

If the account is associated with system commands or applications, the UID shall be changed to a value greater than `0` but less than `1000`.

Rationale

An account has root authority if it has a UID of 0. Multiple accounts with a UID of 0 afford more opportunity for potential intruders to guess a password for a privileged account. Proper configuration of sudo is recommended to afford multiple system administrators access to root privileges in an accountable manner.

bash fix

```
awk -F: '$3 == 0 && $1 != "root" { print $1 }' /etc/passwd | xargs passwd -l &> /dev/null
```

NASA-ASCS-20158: Ensure gpgcheck Enabled for Local Packages

NASA ASCS ID	NASA-ASCS-20158
Severity	**Critical**
Group	software/system
STIG Reference	RHEL_8_STIG RHEL-08-010371
MITRE ATT&CK Reference	T1553, M1028

`Yum` should be configured to verify the signature(s) of local packages prior to installation. To configure `yum` to verify signatures of local packages, set the `localpkg_gpgcheck` to `1` in `/etc/yum.conf` .

Rationale

Changes to any software components can have significant effects to the overall security of the operating system. This requirement ensures the software has not been tampered and 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.

bash fix

```
if which yum &> /dev/null
then
  if grep --silent ^localpkg_gpgcheck /etc/yum.conf ; then
    sed -i "s/^localpkg_gpgcheck.*/localpkg_gpgcheck=1/g" /etc/yum.conf
  else
    echo -e "\n# Set localpkg_gpgcheck to 1 per security requirements" >> /etc/yum.conf
    echo "localpkg_gpgcheck=1" >> /etc/yum.conf
  fi
fi
```

NASA-ASCS-20165: Prevent Login to Accounts With Empty Passwords

NASA ASCS ID	NASA-ASCS-20165
Severity	**Critical**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-020330, RHEL_8_STIG RHEL-08-020331, RHEL_8_STIG RHEL-08-020332
MITRE ATT&CK Reference	TA0006, M1027
MITRE D3FEND Reference	D3-SPP

If an account is configured for password authentication but does not have an assigned password, it may be possible to log into the account without authentication. Remove any instances of the `nullok` option in `/etc/pam.d/system-auth` to prevent logins with empty passwords.

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-update`. Refer to distribution documentation for appropriate configuration use. The PIV-SSSD Handbook has both `authselect` and `pam-auth-update` content that can also help.

Rationale

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

bash fix

```
# NOTE: Use of authselect tool requires System Administrator to fix. See note in specification
document.
```

NASA-ASCS-20235: Enable FIPS Mode at Boot

NASA ASCS ID	NASA-ASCS-20235
Severity	**Critical**
Group	software/system
NIST SP 800-53r5 Reference	SC-13
STIG Reference	RHEL_8_STIG RHEL-08-010020

Ensure the system is running in FIPS mode.

For Red Hat Enterprise 8 Linux systems:

```
fips-mode-setup --enable
```

The `fips-mode-setup` command will configure the system in FIPS mode by automatically configuring the following:

- Setting the kernel FIPS mode flag (`/proc/sys/crypto/fips_enabled`) to `1`
- Creating `/etc/system-fips`
- Setting the system crypto policy in `/etc/crypto-policies/config` to `FIPS`
- Loading the Dracut `fips` module

For SUSE Linux Enterprise:

```
zypper in -t pattern fips
mkinitrd
reboot
```

For Ubuntu:

FIPS booting in Ubuntu requires a Ubuntu Advantage Subscription to have access to tools and libraries needed for enabling this feature.

The following is taken from https://ubuntu.com/security/certifications/docs/fips.

Ensure Ubuntu-Advantage tool is present

```
apt update
apt install ubuntu-advantage-tools
```

Gather token from Ubuntu Advantage subscription via website. Access the licence information at https://ubuntu.com/advantage. Under the license information will be a command with token for the `ua` tool to attach to the system.

Attach license to system

```
ua attach TH15iSN0taT0k4nth15IsN0TaTokAN
```

Enable FIPS updates via the `ua` tool.

```
ua enable fips-updates
```

In some case the FIPS automated updates will prevent use of `LivePatch`

Additional information on kernel parameters can be found here: https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html

Additional information on grub configuration can be found here: https://www.gnu.org/software/grub/manual/grub/html_node/Simple-configuration.html#Simple-configuration

This can not be done automatically, all testing found that automatic updates to this causes system instability. Be cautious in implementing this control in order to get expected results.

Rationale

Use of weak or untested encryption algorithms undermines the purposes of utilizing 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.

bash fix

```
echo "See specific system details on how to enable fips mode in your distribution."
```

NASA-ASCS-20236: The Installed Operating System Is Vendor Supported and Certified

NASA ASCS ID	NASA-ASCS-20236
Severity	**Critical**
Group	software/system
STIG Reference	RHEL_8_STIG RHEL-08-010000

The installed operating system must be maintained and certified by a vendor.

For Red Hat Enterprise Linux, a properly licensed and support system will use the `subscription-manager` application. Status will be used to confirm subscription.

```
subscription-manager identity
```

For Ubuntu operating system, a proper licensed and supported system requires the Ubuntu Pro (or Ubuntu Advantage) subscription along with the `ubuntu-advantage-tools` package installed to register.

```
ua status
```

Ubuntu cloud instances are assumed vendor supported.

For Amazon Linux systems, support is provided with the use of the AWS platform.

For Oracle Linux and Rocky Linux, both are certified for use without fee, the vendor provides paid support if needed.

For Suse Linux Enterprise (SLE) version use `SUSEConnect -s`. The `"subscription_status":"ACTIVE"` value is required.

Rationale

An operating system is considered "supported" if the vendor continues to provide security patches for the product as well as maintain government certification requirements. With an unsupported release, it will not be possible to resolve security issue discovered in the system software as well as meet government certifications.

NASA-ASCS-20240: Uninstall rsh-server Package

NASA ASCS ID	NASA-ASCS-20240
Severity	**Critical**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-040010
MITRE ATT&CK Reference	TA0006, TA0008, M1042

The `rsh-server` package can be uninstalled with the following command:

```
yum remove rsh-server
```

or

```
apt-get purge rsh-server
```

Rationale

The rsh-server service provides unencrypted remote access service. However, it does not provide for the confidentiality and integrity of user passwords or the remote session, and it has very weak authentication. The `rsh-server` package provides several obsolete and insecure network services. Removing it decreases the risk of those services being accidentally (or intentionally) activated.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q rsh-server &> /dev/null
  then
    yum -y remove rsh-server &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' rsh-server )" == "installed" ]]
  then
    apt-get -y purge rsh-server &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q rsh-server &> /dev/null
  then
    zypper --non-interactive remove rsh-server &> /dev/null
  fi
fi
```

NASA-ASCS-20241: Uninstall telnet-server Package

NASA ASCS ID	NASA-ASCS-20241
Severity	**Critical**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-040000
MITRE ATT&CK Reference	TA0006, TA0008, M1042

The `telnet-server` package can be uninstalled with the following command:

```
yum erase telnet-server
```

or

```
apt-get purge telnetd
```

or

```
zypper remove telnet-server
```

Rationale

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities are often overlooked and therefore may remain unsecure. They increase the risk to the platform by providing additional attack vectors. The telnet service provides an unencrypted remote access service which does not provide for the confidentiality and integrity of users' passwords or the remote session. If a privileged user were to log in using this service, the privileged user's password could be compromised. Removing the `telnet-server` package decreases the risk of the telnet service's accidental (or intentional) activation.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q telnet-server &> /dev/null
  then
    yum -y remove telnet-server &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' telnetd )" == "installed" ]]
  then
    apt-get -y purge telnetd &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q telnet-server &> /dev/null
  then
    zypper --non-interactive remove telnet-server &> /dev/null
  fi
fi
```

NASA-ASCS-20244: Uninstall vsftpd Package

NASA ASCS ID	NASA-ASCS-20244
Severity	**Critical**
Group	ftp/services
STIG Reference	RHEL_8_STIG RHEL-08-040360
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 2.2.8
MITRE ATT&CK Reference	TA0001, T1195, TA0003, M1042

The `vsftpd` package can be removed with the following command:

```
yum remove vsftpd
```

or

```
apt-get purge vsftpd
```

or

```
zypper remove vsftpd
```

Rationale

Removing the vsftpd package decreases the risk of it being accidental activation.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q vsftpd &> /dev/null
  then
    yum -y remove vsftpd &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' vsftpd )" == "installed" ]]
  then
    apt-get -y purge vsftpd &> /dev/null
  fi
elif zypper yum &> /dev/null
then
  if rpm -q vsftpd &> /dev/null
  then
    zypper --non-interactive remove vsftpd &> /dev/null
  fi
fi
```

NASA-ASCS-20283: Ensure gpgcheck Enabled For All Package Repositories

NASA ASCS ID	NASA-ASCS-20283
Severity	**Critical**
Group	software/system
NIST SP 800-53r5 Reference	SI-07 (15)
STIG Reference	RHEL_8_STIG RHEL-08-010370, RHEL_8_STIG RHEL-08-010371
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.2.3
MITRE ATT&CK Reference	M1045, T1554

To ensure signature checking is not disabled for any repos.

When using `yum` ensure no entry in `/etc/yum.repos.d/` configuration files have `gpgcheck=0` in them.

When using `apt` ensure no entry in `/etc/apt/sources.list` or `/etc/apt/sources.list.d/` configuration files have trusted, allow-weak, or allow-insecure set to true in them.

When using `zypper` ensure that the defaults are being used by commenting out any lines in `/etc/zypp/zypp.con` related to `gpgcheck`. The `zypper` configuration is set to enforce gpg checks for the metadata, repo, and packages by default.

Rationale

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. Certificates used to verify the software must be from an approved Certificate Authority (CA).

bash fix

```
if which yum &> /dev/null
then
  sed -i "s/gpgcheck=.*/gpgcheck=1/g" /etc/yum.repos.d/*
elif which apt &> /dev/null
then
  sed -i "s/(trusted|allow\-weak|allow\-insecure).*=.*true//g" /etc/apt/sources.list
  sed -i "s/(trusted|allow\-weak|allow\-insecure).*=.*true//g" /etc/apt/sources.list.d/*
elif which zypper &> /dev/null
then
  sed -ir "s/^(\s+)?(gpgcheck.*)$/# \2/I" /etc/zypp/zypp.conf
fi
```

NASA-ASCS-20364: Disable Ctrl-Alt-Del Reboot Activation

NASA ASCS ID	NASA-ASCS-20364
Severity	**Critical**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-040170
MITRE ATT&CK Reference	T1529

By default, `SystemD` will reboot the system if the `Ctrl-Alt-Del` key sequence is pressed.

To configure the system to ignore the `Ctrl-Alt-Del` key sequence from the command line instead of rebooting the system, do either of the following:

```
ln -sf /dev/null /etc/systemd/system/ctrl-alt-del.target
```

or

```
systemctl disable ctrl-alt-del.target
systemctl mask ctrl-alt-del.target
```

Do not simply delete the `/usr/lib/systemd/system/ctrl-alt-del.service` file, as this file may be restored during future system updates.

In systems using `SysV` init, the file `/etc/init/control-alt-delete.conf` contains the `exec` script for management of the `Ctrl-Alt-Del` key sequence.

To configure the `SysV` system to prevent `reboot` on a `Ctrl-Alt-Del` key sequence, comment out the line in the `/etc/init/control-alt-delete.conf` with the `shutdown` command in it.

```
#exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
```

Rationale

A locally logged-in user who presses Ctrl-Alt-Del while at the console can reboot the system. If this key sequence is accidentally pressed, it can result in the loss of availability due to unintentional reboot.

bash fix

```
if which systemctl &> /dev/null
then
  systemctl disable ctrl-alt-del.target &> /dev/null
  systemctl mask ctrl-alt-del.target &> /dev/null
else
  sed -i "s/^exec\ \/sbin\/shutdown/#exec\ \/sbin\/shutdown/" /etc/init/control-alt-delete.conf
  initctl reload-configuration control-alt-delete &> /dev/null
fi
```

NASA-ASCS-20365: Disable Ctrl-Alt-Del Burst Action

NASA ASCS ID	NASA-ASCS-20365
Severity	**Critical**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-040172
MITRE ATT&CK Reference	T1529

By default, `SystemD` will reboot the system if the `Ctrl-Alt-Del` key sequence is pressed more than 7 times in 2 seconds.

To configure the system to ignore the `CtrlAltDelBurstAction` setting, add or modify the following to

`/etc/systemd/system.conf` :

```
CtrlAltDelBurstAction=none
```

Rationale

A locally logged-in user who presses Ctrl-Alt-Del while at the console can reboot the system. If this key sequence is accidentally pressed, it can result in the loss of availability due to unintentional reboot.

bash fix

```
CONFIG_FILE=/etc/systemd/system.conf
EXISTS_IF_REGEX="^CtrlAltDelBurstAction="
SED_INLINE="s/^CtrlAltDelBurstAction=.*$/CtrlAltDelBurstAction=none/"
ECHO_APPEND="CtrlAltDelBurstAction=none"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20366: Remove Host-Based Authentication Files

NASA ASCS ID	NASA-ASCS-20366
Severity	**Critical**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-010460

The `shosts.equiv` file lists remote hosts and users that are trusted by the local system. To remove these files, run the following command to delete them from any location:

```
$ sudo rm /[path]/[to]/[file]/shosts.equiv
```

This control check will time out in 5 minutes to protect system resources, however, it will return a failed result if it times out.

Rationale

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, nor does it require the use of two-factor authentication.

bash fix

```
# NOTE: adding a file to the execution directory called path.exclude will allow an admin
#       to provide a list of locations, each on a single line, to be excluded from the
#       find command that will execute the privileged_commands entry into audit rules.
#       This feature is only for the remediation bash script.
FILTER=""
TIMEOUT=5m
if [ -e path.exclude ]
then
  for LINE in $(<path.exclude)
  do
    FILTER=$FILTER"-path $LINE -o "
  done
  FILTER="${FILTER:0:(-4)} -prune -o"
fi
for DEVTYPE in $( grep -v nodev /proc/filesystems | grep -vE "(fuseblk|squashfs)" )
do
  for MNTPNT in $( findmnt -ln -t $DEVTYPE -o TARGET )
  do
    IFS_BKP="$IFS"
    IFS=$'\n'
    for FILE in $( timeout $TIMEOUT find ${MNTPNT} -maxdepth 3 -xdev \( -type f -o -type l \)
-regex ".*\/\([rs]\)?hosts.equiv")
    do
      rm -f $FILE
    done
    IFS="$IFS_BKP"
  done
done
```

NASA-ASCS-20367: Remove User Host-Based Authentication Files

NASA ASCS ID	NASA-ASCS-20367
Severity	**Critical**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-010470
MITRE ATT&CK Reference	T1078

The `$HOME/.shosts` file (relative to each user's home directory) lists remote hosts and users that are trusted by the local system. To remove these files, run the following command to delete them from any location:

```
$ sudo rm ~/.shosts
```

Rationale

The .shosts 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, nor does it require the use of two-factor authentication.

bash fix

```
for DEVTYPE in $( grep -v nodev /proc/filesystems | grep -vE "(fuseblk|squashfs)" )
do
  for MNTPNT in $( findmnt -ln -t $DEVTYPE -o TARGET )
  do
    find ${MNTPNT} -maxdepth 4 -xdev \( -type f -o -type l \) -regex ".*/\.\([rs]\)?hosts" -exec rm
-f {} \;
  done
done
```

NASA-ASCS-20375: Ensure Local System is Enforcing PIV Authentication

NASA ASCS ID	NASA-ASCS-20375
Severity	**Critical**
Group	accounts/system
NIST SP 800-53r5 Reference	IA-02
STIG Reference	RHEL_8_STIG RHEL-08-020250, RHEL_8_STIG RHEL-08-010400
MITRE ATT&CK Reference	M1032
MITRE D3FEND Reference	D3-MFA

Ensure that the local authentication enforces PIV Multi-Factor Authentication.

This control is similar to control NASA-ASCS-20379 Ensure System is Enforcing Multi-Factor Authentication (MFA).

The Agency provides multiple solutions for providing PIV management in Linux.

The internal website https://cset.nasa.gov/ has links to multiple options regarding PIV solutions at the Agency.

Rationale

NASA requires all systems to be enforcing PIV authentication for all IT assets

NASA-ASCS-20378: Ensure Data at Rest is Implemented

NASA ASCS ID	NASA-ASCS-20378
Severity	**Critical**

Group	encryption
NIST SP 800-53r5 Reference	SC-28, IA-07, SC-13
STIG Reference	RHEL_8_STIG RHEL-08-010030, RHEL_8_STIG RHEL-08-010020
MITRE ATT&CK Reference	M1057
MITRE D3FEND Reference	D3-DENCR

Ensure all volumes are encrypted.

Rationale

Unencrypted volumes on a system can be easily bypassed if physically accessible

NASA-ASCS-40038: (OpenSSH) Use Only Approved Ciphers

NASA ASCS ID	NASA-ASCS-40038
Severity	**Critical**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-08 (1), IA-07, AC-17 (2)
STIG Reference	RHEL_8_STIG RHEL-08-010291
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENCR
Control Setting	aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

This setting specifies which ciphers are allowed.

To configure the setting for OpenSSH, insert the OS-specific value into the following line and then add or correct this line in the `sshd_config` file on the system:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

The FIPS 140 validated, OS-specific values are defined in the ASCS Specification for each OS.

Rationale

Weak ciphers have been to shown to have potential and documented exploits that can lead to system compromise or communication interception.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^Ciphers"
SED_INLINE="s/^Ciphers.*$/Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-
gcm@openssh.com/"
ECHO_APPEND="Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-
gcm@openssh.com"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40052: (OpenSSH) Use Only Strong Key Exchange Algorithms

NASA ASCS ID	NASA-ASCS-40052
Severity	**Critical**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-08 (1), IA-07, AC-17 (2)
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENRC
Control Setting	ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512

This setting specifies the available Key Exchange (KEX) algorithms.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
KexAlgorithms ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512
```

The FIPS 140 validated, OS-specific values are defined in the ASCS Specification for each OS.

Rationale

Use of weak KEX algorithms has been shown to allow attacks on the initial connection of SSH. A compromised KEX would allow for a man-in-the-middle attack.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^KexAlgorithms"
SED_INLINE="s/^KexAlgorithms.*$/KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512/"
ECHO_APPEND="KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40056: (OpenSSH) Use Only Strong Hashing Algorithms for MACs

NASA ASCS ID	NASA-ASCS-40056
Severity	**Critical**

Group	ssh/services
NIST SP 800-53r5 Reference	SC-08 (1), AC-17 (2), IA-07
STIG Reference	RHEL_8_STIG RHEL-08-010290
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENCR
Control Setting	hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com

This setting specifies the available Message Authentication Code (MAC) algorithms. The MAC algorithm is used for data integrity protection.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
MACs hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com
```

The FIPS 140 validated, OS-specific values are defined in the ASCS Specification for each OS.

Rationale

The MAC algorithm is used to ensure packet integrity. Use of weak hashing algorithms can compromise messages using collision techniques, preventing the integrity of a packet from being ensured.

bash fix

```
[[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
[[ $(uname) == "Darwin" ]] && SEDINLINE="s/^.*MACs.*" || SEDINLINE="s/^\(\s\+\)\?MACs\s.*$"
if grep -E "^(\s+)?MACs\s" $CONFIG_FILE &> /dev/null
then
  sed -i.bak "$SEDINLINE/MACs\ hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm@openssh.com,hmac-sha2-
512-etm@openssh.com/" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
else
  echo "MACs hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
etm@openssh.com" >> $CONFIG_FILE
fi
```

NASA-ASCS-40061: (OpenSSH) Disable SSH Access via Empty Passwords

NASA ASCS ID	NASA-ASCS-40061
Severity	**Critical**
Group	ssh/services

STIG Reference	RHEL_8_STIG RHEL-08-020330
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.9
MITRE ATT&CK Reference	TA0006, M1027
MITRE D3FEND Reference	D3-SPP
Control Setting	no

When password authentication is allowed, this setting specifies whether the server allows login to accounts with empty password strings.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PermitEmptyPasswords no
```

Rationale

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

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PermitEmptyPasswords"
SED_INLINE="s/^PermitEmptyPasswords.*$/PermitEmptyPasswords no/"
ECHO_APPEND="PermitEmptyPasswords no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40068: (OpenSSH) Allow Only SSH Protocol 2

NASA ASCS ID	NASA-ASCS-40068
Severity	**Critical**
Group	ssh/services
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.8
MITRE ATT&CK Reference	M1042
Control Setting	2

This setting specifies which protocol version is to be used by `sshd`.

The setting `Protocol` has been deprecated since version 7.4p1. Adding the setting will cause `sshd` to generate unwanted log messages.

To configure the setting for OpenSSH in versions prior to 7.4p1, add or correct the following line in the sshd_config file on the system:

```
Protocol 2
```

Rationale

SSH protocol version 1 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.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^Protocol"
SED_INLINE="s/^Protocol.*$/Protocol 2/"
ECHO_APPEND="Protocol 2"

if [[ "$( sshd -T -C user=root -C host=localhost -C addr=localhost | grep protocol )" != "" ]]
then
  INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
  if ls $INCLUDES &> /dev/null
  then
    CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
  fi
  FIXED=1
  for CONFIG_FILE in ${CONFFILES[*]}
  do
    if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
    then
      sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
      FIXED=0
    fi
  done
```

```
  if [[ "$FIXED" != "0" ]]
  then
    [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-40069: (OpenSSH) Use Only Strong Public Key Types

NASA ASCS ID	NASA-ASCS-40069
Severity	**Critical**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-08 (1), IA-07, AC-17 (2)
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENRC

This setting specifies the key types that will be accepted for public key authentication as a comma-separated pattern list.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PubkeyAcceptedKeyTypes <COMMA DELIMITED LIST OF KEY OPTIONS>
```

Current Accepted Keys (may not all be available depending on OS and release):

- ssh-ed25519
- ssh-ed25519-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-rsa
- rsa-sha2-512
- rsa-sha2-256

The FIPS 140 validated, OS-specific values are defined in the ASCS Specification for each OS.

As of OpenSSH v8.5p1, the `PubkeyAcceptedTypes` keyword has been renamed to `PubkeyAcceptedAlgorithms`.

Rationale

The public key is used after the key exchange to authenticate the connecting party. With use of weak public keys there is a potential to be able to determine the private key.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PubkeyAcceptedKeyTypes"
SEDINLINE="s/^PubkeyAcceptedKeyTypes.*"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SEDINLINE/PubkeyAcceptedKeyTypes\ ssh-ed25519,ssh-ed25519-cert-
v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-
v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-
nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256/" $CONFIG_FILE;
rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo "PubkeyAcceptedKeyTypes ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-
cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-
nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256" >> $CONFIG_FILE
fi
```

NASA-ASCS-40558: (Linux Desktop) Disable Automatic Login

NASA ASCS ID	NASA-ASCS-40558
Severity	**Critical**

Group	software/displaymanager
STIG Reference	RHEL_8_STIG RHEL-08-010820
MITRE ATT&CK Reference	TA0006, M1043
MITRE D3FEND Reference	D3-SSP

Display Managers can allow users to automatically log in without user interaction or credentials. However, this is insecure. Therefore, users should always be required to authenticate themselves to the system that they are authorized to use.

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40561: (Linux Desktop) Disable Ctrl-Alt-Del Reboot Key Sequence in GUI

NASA ASCS ID	NASA-ASCS-40561
Severity	**Critical**
Group	software/system
STIG Reference	RHEL_8_STIG RHEL-08-040171
MITRE ATT&CK Reference	T1529

Configure the desktop environment to ignore the `Ctrl-Alt-Del` key sequence.

See [_configuration_options] for remediation guides for desktop environments and display managers.

Rationale

A locally logged-in user who presses Ctrl-Alt-Del while at the console can reboot the system. If this key sequence is accidentally pressed, it can result in the loss of availability due to an unintentional reboot.

NASA-ASCS-40682: (OpenSSH) Configure Remote Access for PIV

NASA ASCS ID	NASA-ASCS-40682
Severity	**Critical**
Group	ssh/auth
NIST SP 800-53r5 Reference	IA-02
MITRE ATT&CK Reference	M1032

MITRE D3FEND Reference	D3-MFA

Configure OpenSSH to enforce Multi-Factor Authentication (MFA) for remote access using a PIV.

See CSET's Handbooks for supporting guidance on how to configure PIV solutions on specific platforms.

Rationale

NASA requires all systems to enforce PIV authentication for access to all IT assets.

5.2. High Severity Settings

High severity settings ***SHALL*** be adhered to, as they are monitored, scored, and reported to NASA.

- *High* severity settings target any vulnerability which, if exploited, would directly and immediately result in the loss of confidentiality, integrity, or availability.
- Deviations from *high* severity settings require approval from the NASA CIO or CIO designee.

NASA-ASCS-20003: Set Password Minimum Length

NASA ASCS ID	NASA-ASCS-20003
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	IA-05
STIG Reference	RHEL_8_STIG RHEL-08-020230
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.5.1
MITRE ATT&CK Reference	TA0006, T1110, M1027
Control Setting	8

Set the `pwquality minlen` value to 8 or greater.

This can be accomplished using the `/etc/security/pwquality.conf` entry or the `pam_pwquality` pam line directly in the `/etc/pam.d` configurations. **It is recommended to use the `/etc/security/pwquality.conf` file over inline `/etc/pam.d/` configuration.**

If using the `/etc/security/pwquality.conf` file for this control, use it also on control 20126 (retry attempts), do not mix it with using cracklib or pam_pwquality in the pam files.

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-`

> `update`. Refer to distribution documentation for appropriate configuration use.

Rationale

NIST 800-63 provides explanation of the choice of current password length restrictions. From NIST SP 800-63: "Length and complexity requirements beyond those recommended here significantly increase the difficulty of memorized secrets and increase user frustration. As a result, users often work around these restrictions in a way that is counterproductive. Furthermore, other mitigations such as blacklists, secure hashed storage, and rate limiting are more effective at preventing modern brute-force attacks. Therefore, no additional complexity requirements are imposed."

bash fix

```
if [ -f /etc/security/pwquality.conf ]
then
  VAL=$(grep -E "^(\s+)?minlen" /etc/security/pwquality.conf | sed -e "s/\s\+//g" | cut -d= -f2)
  if ! [ $VAL ]
  then
    echo "minlen = 8" >> /etc/security/pwquality.conf
  elif [[ "$VAL" -lt "8" ]]
  then
    sed -i "s/^minlen.*$/minlen\ =\ 8/" /etc/security/pwquality.conf
  fi
else
  echo "Remediation only considers /etc/security/pwquality.conf used in modern linux versions."
fi
```

NASA-ASCS-20009: System Audit Logs Must Have Mode 0640 or Less Permissive

NASA ASCS ID	NASA-ASCS-20009
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-09, AC-03 (4)
STIG Reference	RHEL_8_STIG RHEL-08-030120
MITRE ATT&CK Reference	T1564
MITRE D3FEND Reference	D3-LFP, D3-SCP

Files associated to `auditd` shall only allow owner to read and write and group to read. All files associated with `auditd` in `/var/log/audit` shall maintain the proper permissions. Archived audit files shall be set to read only.

```
chmod 0640 /var/log/audit/audit.log
chmod 0440 /var/log/audit/audit.log.*
```

Rationale

If users can write to audit logs, audit trails can be modified or destroyed.

bash fix

```
chmod 0640 /var/log/audit/audit.log
chmod 0440 /var/log/audit/audit.log.*
```

NASA-ASCS-20012: Disallow Direct root Logins

NASA ASCS ID	NASA-ASCS-20012
Severity	**High**
Group	accounts/system
MITRE ATT&CK Reference	T1078.001
MITRE D3FEND Reference	D3-AM

To further limit access to the `root` account, disable root logins at the console by editing the `/etc/securetty` file. This file lists all devices that the root user is allowed to access. If the file does not exist at all, the root user can access through any communication method on the system, whether via the console or via a raw network interface.

To prevent root from logging in, ensure the /etc/securetty file exists and remove its contents.

The following command will remove the contents of the file or create an empty version of it:

```
$ echo > /etc/securetty
```

To provide an alternative to using `root` account access, CSET has provided the Linux Emergency Access Account Supplemental Handbook to assist administrators in setting up a isolated alternative account.

If the root account is completely locked out, the `/etc/securetty` feature does not have to be enabled. We recommend that it is installed and enabled regardless, but recognise that complete root lock out is sufficient for meeting this control.

In newer distributions, such as RHEL 8 and Ubuntu 20.04, the `securetty` feature is no longer default and the `pam_securetty.so` element must be added to the `login` and `remote` configuration of `/etc/pam.d`

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-update`. Refer to distribution documentation for appropriate configuration use.

Rationale

Disabling direct root logins ensures proper accountability and multifactor authentication to privileged accounts. Users will first log in, then escalate to privileged (root) access via su / sudo.

bash fix

```
PAMS=""
if [[ "$OS_LIKE" == "fedora" ]]
then
  if [[ "$( grep -vE "^(\s+)?#" /etc/pam.d/login | grep securetty )" == "" ]]
  then
    FIRST=/bin/true

    IFS_BKP="$IFS"; IFS=$'\n'; for LINE in $(</etc/pam.d/login)
    do
      if [[ "$( echo $LINE | grep -E "^(\s+)?#" )" == "" ]]
      then
        if $FIRST
        then
          echo "auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so"
>> /tmp/pam.d-login-tmp
          FIRST=/bin/false
        fi
      fi
      echo $LINE >> /tmp/pam.d-login-tmp
    done; IFS="$IFS_BKP"
    cp -a /etc/pam.d/login /etc/pam.d/login.fixtext.backup
    cp /tmp/pam.d-login-tmp /etc/pam.d/login
    rm /tmp/pam.d-login-tmp
  fi
  if [[ "$( grep -vE "^(\s+)?#" /etc/pam.d/remote | grep securetty )" == "" ]]
  then
    FIRST=/bin/true
    IFS_BKP="$IFS"; IFS=$'\n'; for LINE in $(</etc/pam.d/remote)
    do
      if [[ "$( echo $LINE | grep -E "^(\s+)?#" )" == "" ]]
      then
        if $FIRST
        then
          echo "auth       required     pam_securetty.so" >> /tmp/pam.d-remote-tmp
          FIRST=/bin/false
        fi
      fi
      echo $LINE >> /tmp/pam.d-remote-tmp
    done; IFS="$IFS_BKP"
    cp -a /etc/pam.d/remote /etc/pam.d/remote.fixtext.backup
    cp /tmp/pam.d-remote-tmp /etc/pam.d/remote
    rm /tmp/pam.d-remote-tmp
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( grep -vE "^(\s+)?#" /etc/pam.d/login | grep securetty )" == "" ]]
  then
    IFS_BKP="$IFS"; IFS=$'\n'; for LINE in $(</etc/pam.d/login)
```

```
    do
      if [[ "$( echo $LINE | grep -vE "^(\s+)?#" | grep faildelay )" != "" ]]
      then
        echo $LINE >> /tmp/pam.d-login-tmp
        echo "auth [success=ok new_authtok_reqd=ok ignore=ignore user_unknown=bad default=die]
pam_securetty.so" >> /tmp/pam.d-login-tmp
      else
        echo $LINE >> /tmp/pam.d-login-tmp
      fi
    done; IFS="$IFS_BKP"
    cp -a /etc/pam.d/login /etc/pam.d/login.fixtext.backup
    cp /tmp/pam.d-login-tmp /etc/pam.d/login
    rm /tmp/pam.d-login-tmp
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if [[ "$( grep -vE "^(\s+)?#" /etc/pam.d/login | grep securetty )" == "" ]]
  then
    FIRST=/bin/true

    IFS_BKP="$IFS"; IFS=$'\n'; for LINE in $(</etc/pam.d/login)
    do
      if [[ "$( echo $LINE | grep -E "^(\s+)?#" )" == "" ]]
      then
        if $FIRST
        then
          echo "auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so"
>> /tmp/pam.d-login-tmp
          FIRST=/bin/false
        fi
      fi
      echo $LINE >> /tmp/pam.d-login-tmp
    done; IFS="$IFS_BKP"
    cp -a /etc/pam.d/login /etc/pam.d/login.fixtext.backup
    cp /tmp/pam.d-login-tmp /etc/pam.d/login
    rm /tmp/pam.d-login-tmp
  fi
  if [[ "$( grep -vE "^(\s+)?#" /etc/pam.d/remote | grep securetty )" == "" ]]
  then
    FIRST=/bin/true
    IFS_BKP="$IFS"; IFS=$'\n'; for LINE in $(</etc/pam.d/remote)
    do
      if [[ "$( echo $LINE | grep -E "^(\s+)?#" )" == "" ]]
      then
        if $FIRST
        then
          echo "auth       required     pam_securetty.so" >> /tmp/pam.d-remote-tmp
          FIRST=/bin/false
        fi
      fi
      echo $LINE >> /tmp/pam.d-remote-tmp
    done; IFS="$IFS_BKP"
```

```
    cp -a /etc/pam.d/remote /etc/pam.d/remote.fixtext.backup
    cp /tmp/pam.d-remote-tmp /etc/pam.d/remote
    rm /tmp/pam.d-remote-tmp
  fi
fi

echo > /etc/securetty
```

NASA-ASCS-20020: Verify All Account Password Hashes are Shadowed

NASA ASCS ID	NASA-ASCS-20020
Severity	**High**
Group	accounts/system
MITRE ATT&CK Reference	T1078, M1027
MITRE D3FEND Reference	D3-CCSA

If any password hashes are stored in `/etc/passwd` (in the second field, instead of an `x` or `*`), the cause of this misconfiguration shall be investigated. The account shall have its password reset and the hash shall be properly stored, or the account shall be deleted entirely.

Rationale

The hashes for all user account passwords shall be stored in the file /etc/shadow and never in /etc/passwd, which is readable by all users.

NASA-ASCS-20024: Ensure auditd Collects File Deletion Events by User

NASA ASCS ID	NASA-ASCS-20024
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030361
MITRE ATT&CK Reference	T1070.002, DS0022
MITRE D3FEND Reference	D3-SFA

Collect file deletion events for all users and root. The audit trail could aid in system troubleshooting, as well as detecting malicious processes that attempt to delete log files to conceal their presence.

The auditd daemon is configured to use the augenrules program to read audit rules during daemon startup (the default), add the following lines to a file with suffix .rules in the directory /etc/audit/rules.d, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S rmdir,unlink,unlinkat,rename,renameat,renameat2 -F auid>=1000 -F
auid!=4294967295 -F key=file_deletion_events
-a always,exit -F arch=b64 -S rmdir,unlink,unlinkat,rename,renameat,renameat2 -F auid>=1000 -F
auid!=4294967295 -F key=file_deletion_events
```

The -F key= or -k flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

The auid value shown as 4294967295 may appear on inspection of the control as either -1 or unset, this is a valid return and all the values have the same meaning to auditd.

Rationale

Auditing file deletions will create an audit trail for files that are removed from the system.

bash fix

```
ARCHS=(b64 b32)
for ARCH in ${ARCHS[*]}
do
  SLIST=(rmdir unlink unlinkat rename renameat renameat2 )

  for SITEM in ${SLIST[*]}
  do
    if [ ! "$( grep -E -- "-S\s([a-zA-Z0-9_,]*)\b$SITEM\b(,)?([a-zA-Z0-9_,]*)?\s"
/etc/audit/rules.d/* | grep -- "-F arch=$ARCH" )" ]
    then
      echo "-a always,exit -F arch=$ARCH -S $SITEM -F auid>=1000 -F auid!=4294967295 -F
key=file_deletion_events" >> /etc/audit/rules.d/40-file_delete_event.rules
    fi
  done
done
```

NASA-ASCS-20025: Make the auditd Configuration Immutable

NASA ASCS ID	NASA-ASCS-20025
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-09
STIG Reference	RHEL_8_STIG RHEL-08-030121

CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.20
MITRE ATT&CK Reference	TA0005, T1564, T1562, M1047
MITRE D3FEND Reference	D3-SCP

Set the `auditd` configuration to be immutable to prevent malicious or accidental rule changes.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`.

```
-e 2
```

With this setting, a reboot will be required to change any audit rules.

Rationale

Making the audit configuration immutable prevents accidental as well as malicious modification of the audit rules, although it may be problematic if legitimate changes are needed during system operation.

NASA-ASCS-20026: Ensure auditd Collects Information on Kernel Module Loading and Unloading

NASA ASCS ID	NASA-ASCS-20026
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030360, RHEL_8_STIG RHEL-08-030390
MITRE ATT&CK Reference	DS0008
MITRE D3FEND Reference	D3-OSM

To capture kernel module loading and unloading events.

For older version of Linux the module loading and unloading is done via individual files, for newer versions the work is done by a single application `kmod`.

Depending on the distribution, the location of `kmod` may be in either `/bin/kmod` or `/usr/bin/kmod`. The use of the `which kmod` command will show the location. The check will attempt to find the non-symlinked location of the file for use with the audit rules. Another method would be to use the `find` command along with the `root` users `PATH` value. `find ${PATH//:/ } -name kmod`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-w /usr/bin/kmod -p x -F key=modules
-a always,exit -F arch=b32 -S create_module,init_module,delete_module,finit_module -F key=modules
-a always,exit -F arch=b64 -S create_module,init_module,delete_module,finit_module -F key=modules
```

Audit also when `kexec_load` is implemented on the system

```
-a always,exit -F arch=b32 -S sys_kexec_load -F key=KEXEC
-a always,exit -F arch=b64 -S kexec_load -F key=KEXEC
```

Additionally, monitor important kernel configuration files for changes.

The `sys_kexec_load` and `kexec_load` actions are only checked if the `sysctl` flag is set to allow kexec. The output for `sysctl -n kernel.kexec_load_disabled` should be a 1 if disabled.

```
-w /etc/sysctl.conf -p wa -F key=sysctl
-w /etc/sysctl.d -p wa -F key=sysctl
-w /etc/modprobe.conf -p wa -F key=modprobe
-w /etc/modprobe.d -p wa -F key=modprobe
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The addition/removal of kernel modules can be used to alter the behavior of the kernel and potentially introduce malicious code into kernel space. It is important to have an audit trail of modules that have been introduced into the kernel.

bash fix

```
if [[ "$( stat -c "%F" $(which modprobe) )" == "symbolic link" ]]
then
  WLIST=(kmod)
else
  WLIST=(insmod rmmod modprobe)
fi
for w in ${WLIST[*]}
do
  for FILE in $( find ${PATH//:/ } -name $w 2> /dev/null )
  do
    TARGET=$( echo $FILE | sed "s/\//\\\\\//g" )
    if [ ! "$( grep -E "\-w\s${TARGET}" /etc/audit/rules.d/*)" ]
    then
      echo "-w $FILE -p x -F key=kernel_module_loading" >> /etc/audit/rules.d/05-
kernel_module.rules
```

```
    fi
  done
done

ARCHS=(b32 b64)
CONTROLS=(create_module init_module delete_module finit_module)
for CONTROL in ${CONTROLS[*]}
do
  for ARCH in ${ARCHS[*]}
  do
    if [ ! "$( grep -E -- "-S([a-zA-Z0-9,_ -]*)?\b$CONTROL\b([a-zA-Z0-9,_ -]*)?"
/etc/audit/rules.d/* | grep -E -- "-F\sarch=$ARCH" )" ]
    then
      echo "-a always,exit -F arch=$ARCH -S $CONTROL -F key=kernel_module_loading" >>
/etc/audit/rules.d/05-kernel_module.rules
    fi
  done
done

FILELIST=("/etc/sysctl.d" "/etc/sysctl.conf" "/etc/modprobe.conf" "/etc/modprobe.d" )
for FILE in ${FILELIST[*]}
do
  if [ ! "$( grep -- "-w $FILE[ |$]" /etc/audit/rules.d/* | grep -vE "^\s*#" | grep -E -- "-p\s*wa"
)" ]
  then
    echo "-w $FILE -p wa -F key=kernel_module_loading" >> /etc/audit/rules.d/05-kernel_module.rules
  fi
done

if [ "$( sysctl -n kernel.kexec_load_disabled )" -ne "1" ]
then
  if [ ! "$( grep -E -- "-S([a-zA-Z0-9,_ -]*)?\bsys_kexec_load\b([a-zA-Z0-9,_ -]*)?"
/etc/audit/rules.d/* )" ]
  then
    echo "-a always,exit -F arch=b32 -S sys_kexec_load -F key=KEXEC" >> /etc/audit/rules.d/05-
kernel_module.rules
  fi
  if [ ! "$( grep -E -- "-S([a-zA-Z0-9,_ -]*)?\bkexec_load\b([a-zA-Z0-9,_ -]*)?"
/etc/audit/rules.d/* )" ]
  then
    echo "-a always,exit -F arch=b64 -S kexec_load -F key=KEXEC" >> /etc/audit/rules.d/05-
kernel_module.rules
  fi
fi
```

NASA-ASCS-20027: Record Events that Modify the System Mandatory Access Controls (MAC)

NASA ASCS ID	NASA-ASCS-20027

Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM

Monitor any changes to the Mandatory Access Control (MAC) policies.

If the `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following line to a file with suffix `.rules` in the directory `/etc/audit/rules.d` :

For systems using SELinux:

```
-w /etc/selinux/ -p wa -F key=MAC-policy
```

For systems using AppArmor:

```
-w /etc/apparmor/ -p wa -F key=MAC-policy
-w /etc/apparmor.d/ -p wa -F key=MAC-policy
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The system's MAC policies should not be arbitrarily changed by anything other than administrator action. All changes to MAC policy should be audited.

bash fix

```
if which sestatus &> /dev/null
then
  if [ ! "$( grep -vE "^\s*#" /etc/audit/rules.d/* | grep -E -- "-p\s+wa" | grep -E "\-
w\s+\/etc\/selinux(\/)?(\s|$)" )" ]
  then
    echo "-w /etc/selinux -p wa -F key=mac_modification" >> /etc/audit/rules.d/30-
mac_controls.rules
  fi
elif which aa-status &> /dev/null
then
  if [ ! "$( grep -vE "^\s*#" /etc/audit/rules.d/* | grep -E -- "-p\s+wa" | grep -E "\-
w\s+\/etc\/apparmor(\/)?(\s|$)" )" ]
  then
    echo "-w /etc/apparmor -p wa -F key=mac_modification" >> /etc/audit/rules.d/30-
mac_controls.rules
  fi
```

```
  if [ ! "$( grep -vE "^\s*#" /etc/audit/rules.d/* | grep -E -- "-p\s+wa" | grep -E "\-
w\s+\/etc\/apparmor\.d(\/)?(\s|$)" )" ]
  then
    echo "-w /etc/apparmor.d -p wa -F key=mac_modification" >> /etc/audit/rules.d/30-
mac_controls.rules
  fi
fi
```

NASA-ASCS-20028: Record Events that Modify the System Network Environment

NASA ASCS ID	NASA-ASCS-20028
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.5
MITRE ATT&CK Reference	T1557, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all changes to network configurations.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=networkconfig_modification
-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=networkconfig_modification
```

Additionally, the files related to network configurations are also added to the `/etc/audit/rules.d` directory.

RHEL Based systems

```
-w /etc/issue -p wa -F key=networkconfig_modification
-w /etc/issue.net -p wa -F key=networkconfig_modification
-w /etc/hosts -p wa -F key=networkconfig_modification
-w /etc/sysconfig/network -p wa -F key=networkconfig_modification
-w /etc/sysconfig/network-scripts/ -p wa -F key=networkconfig_modification
```

Ubuntu Based systems

```
-w /etc/issue -p wa -F key=networkconfig_modification
-w /etc/issue.net -p wa -F key=networkconfig_modification
-w /etc/hosts -p wa -F key=networkconfig_modification
```

```
-w /etc/network -p wa -F key=networkconfig_modification
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The network environment shall not be modified by anything other than administrator action. Any change to network parameters shall be audited.

bash fix

```
for ACTION in sethostname setdomainname
do
  if ! grep -E "$ACTION" /etc/audit/rules.d/* | grep -vE "\s*#" &> /dev/null
  then
    echo "-a always,exit -F arch=b32 -S $ACTION -F key=networkconfig_modification" >>
/etc/audit/rules.d/25-network_mods.rules
    echo "-a always,exit -F arch=b64 -S $ACTION -F key=networkconfig_modification" >>
/etc/audit/rules.d/25-network_mods.rules
  fi
done

for FILE in /etc/issue /etc/issue.net /etc/hosts /etc/network /etc/sysconfig/network
/etc/sysconfig/network-scripts
do
  if [ -e $FILE ]
  then
    if ! grep -- "-w $FILE[ |$]" /etc/audit/rules.d/* | grep -vE "\s*#" &> /dev/null
    then
      echo "-w $FILE -p wa -F key=networkconfig_modification" >> /etc/audit/rules.d/25-
network_mods.rules
    fi
  fi
done
```

NASA-ASCS-20029: Record Attempts to Alter Time Through adjtimex

NASA ASCS ID	NASA-ASCS-20029
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.4
MITRE ATT&CK Reference	TA0005, T1562, M1047

MITRE D3FEND Reference	D3-OSM

Monitor clock changes that use the `adjtimex` system call.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S adjtimex -F key=audit_time_rules
-a always,exit -F arch=b64 -S adjtimex -F key=audit_time_rules
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

Arbitrary changes to the system time can be used to obfuscate nefarious activities in log files, as well as to confuse network services (such as sshd) that are highly dependent upon the accurate system time. All changes to the system time shall be audited.

bash fix

```
CONTROL="adjtimex"
for ARCH in b32 b64
do
  if [ ! "$( grep -E -- "-S\s([a-zA-Z0-9_,]*)\b$CONTROL\b(,)?" /etc/audit/rules.d/* | grep -E -- "-
a\salways" | grep -- "-F arch=$ARCH" )" ]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F key=audit_time_rules" >>
/etc/audit/rules.d/10-clock_changes.rules
  fi
done
```

NASA-ASCS-20030: Record Attempts to Alter Time Through clock_settime

NASA ASCS ID	NASA-ASCS-20030
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.4
MITRE ATT&CK Reference	TA0005, T1562, M1047

MITRE D3FEND Reference	D3-OSM

Monitor clock changes using the `clock_settime` system call.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S clock_settime -F key=audit_time_rules
-a always,exit -F arch=b64 -S clock_settime -F key=audit_time_rules
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

Arbitrary changes to the system time can be used to obfuscate nefarious activities in log files, as well as to confuse network services (such as sshd) that are highly dependent upon an accurate system time. All changes to the system time shall be audited.

bash fix

```
ARCHS=(b32 b64)
CONTROL="clock_settime"

for ARCH in ${ARCHS[*]}
do
  if [ ! "$( grep -E -- "-S\s([a-zA-Z0-9_,]*)\b$CONTROL\b(,)?([a-zA-Z0-9_,]*)?\s"
/etc/audit/rules.d/* | grep -- "-F arch=$ARCH" )" ]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F key=audit_time_rules" >>
/etc/audit/rules.d/10-clock_changes.rules
  fi
done
```

NASA-ASCS-20031: Record Attempts to Alter Time Through settimeofday

NASA ASCS ID	NASA-ASCS-20031
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.4

MITRE ATT&CK Reference	TA0005, T1562, M1047
MITRE D3FEND Reference	D3-OSM

Monitor clock changes that use the `settimeofday` system call.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S settimeofday -F key=audit_time_rules
-a always,exit -F arch=b64 -S settimeofday -F key=audit_time_rules
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

Arbitrary changes to the system time can be used to obfuscate nefarious activities in log files, as well as to confuse network services (such as sshd) that are highly dependent upon the accurate system time. All changes to the system time shall be audited.

bash fix

```
ARCHS=(b32 b64)
CONTROL="settimeofday"

for ARCH in ${ARCHS[*]}
do
  if [ ! "$( grep -E -- "-S\s([a-zA-Z0-9_,]*)\b$CONTROL\b(,)?([a-zA-Z0-9_,]*)?\s"
/etc/audit/rules.d/* | grep -- "-F arch=$ARCH" )" ]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F key=audit_time_rules" >>
/etc/audit/rules.d/10-clock_changes.rules
  fi
done
```

NASA-ASCS-20033: Record Attempts to Alter the localtime File

NASA ASCS ID	NASA-ASCS-20033
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)

CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.4
MITRE ATT&CK Reference	TA0005, T1562, M1047
MITRE D3FEND Reference	D3-OSM

Monitor the `/etc/localtime` file for modification.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`:

```
-w /etc/localtime -p wa -F key=audit_time_rules
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

Arbitrary changes to the system time can be used to obfuscate nefarious activities in log files, as well as to confuse network services (such as sshd) that are highly dependent upon the accurate system time. All changes to the system time shall be audited.

bash fix

```
if [ ! "$( grep -E -- "-w\s+\/etc\/localtime(\s|$)" /etc/audit/rules.d/* )" ]
then
  echo "-w /etc/localtime -p wa -F key=audit_time_rules" >> /etc/audit/rules.d/10-
clock_changes.rules
fi
```

NASA-ASCS-20034: Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)

NASA ASCS ID	NASA-ASCS-20034
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030420, RHEL_8_STIG RHEL-08-030490, RHEL_8_STIG RHEL-08-030480, RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.7
MITRE ATT&CK Reference	TA0005, T1564, T1485, T1562, T1562.006, M1047

MITRE D3FEND Reference	D3-OSM

Monitor all unauthorized attempts to change file.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-
EACCES -F auid>=1000 -F auid!=4294967295 -F key=access
-a always,exit -F arch=b32 -S creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM
-F auid>=1000 -F auid!=4294967295 -F key=access
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F a2&0100 -F exit=-EACCES -F
auid>=1000 -F auid!=4294967295 -F key=unsuccessful-create
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F a2&0100 -F exit=-EPERM -F auid>=1000
-F auid!=4294967295 -F key=unsuccessful-create
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F a2&01003 -F exit=-EACCES -F
auid>=1000 -F auid!=4294967295 -F key=unsuccessful-modification
-a always,exit -F arch=b32 -S open,openat,open_by_handle_at -F a2&01003 -F exit=-EPERM -F
auid>=1000 -F auid!=4294967295 -F key=unsuccessful-modification
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

Unsuccessful attempts to access files could be an indicator of malicious activity on a system. Auditing these events could serve as evidence of potential system compromise.

bash fix

```
ARCHS=(b32 b64)
for ARCH in ${ARCHS[*]}
do
  TYPES=(EPERM EACCES)
  for TYPE in ${TYPES[*]}
  do
    ALIST=(creat open openat open_by_handle_at truncate ftruncate)
    for AITEM in ${ALIST[*]}
    do
      if [ ! "$( grep -E -- "-S([a-zA-Z0-9_, ]*)?\b$AITEM\b(,)?" /etc/audit/rules.d/* | grep -E --
"-F\sexit=-$TYPE(\s|$)" | grep -E -- "-F\sarch=$ARCH" )" ]
      then
        echo "-a always,exit -F arch=$ARCH -S $AITEM -F exit=-$TYPE -F auid>=1000 -F
auid!=4294967295 -F key=access" >> /etc/audit/rules.d/45-unsuccess_file_mods.rules
      fi
```

```
    done

    CLIST=(open openat open_by_handle_at)
    for CITEM in ${CLIST[*]}
    do
      if [ ! "$( grep -E -- "-S([a-zA-Z0-9_, ]*)?\b$CITEM\b(,)?" /etc/audit/rules.d/* | grep -E --
"-F\sexit=-$TYPE(\s|$)" | grep -E "a2&0100(\s|$)" | grep -E -- "-F\sarch=$ARCH" )" ]
      then
        echo "-a always,exit -F arch=$ARCH -S $CITEM -F a2&0100 -F exit=-$TYPE -F auid>=1000 -F
auid!=4294967295 -F key=unsuccessful-create" >> /etc/audit/rules.d/45-unsuccess_file_mods.rules
      fi
    done

    UMLIST=(open openat open_by_handle_at)
    for UMITEM in ${UMLIST[*]}
    do
      if [ ! "$( grep -E -- "-S([a-zA-Z0-9_, ]*)?\b$UMITEM\b(,)?" /etc/audit/rules.d/* | grep -E --
"-F\sexit=-$TYPE(\s|$)" | grep -E "a2&01003(\s|$)" | grep -E -- "-F\sarch=$ARCH" )" ]
      then
        echo "-a always,exit -F arch=$ARCH -S $UMITEM -F a2&01003 -F exit=-$TYPE -F auid>=1000 -F
auid!=4294967295 -F key=unsuccessful-modification" >> /etc/audit/rules.d/45-
unsuccess_file_mods.rules
      fi
    done
  done
done
```

NASA-ASCS-20036: Modify the System Login Banner

NASA ASCS ID	NASA-ASCS-20036
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-08
STIG Reference	RHEL_8_STIG RHEL-08-010060
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.7.2

Control Setting	By[\s\n]accessing[\s\n]+and[\s\n]+using[\s\n]+this[\s\n]+information[\s\n]+system\,[\s\n]+you[\s\n]+acknowledge[\s\n]+and[\s\n]+consent[\s\n]+to[\s\n]+the[\s\n]+following:[\s\n]*[\s\n]*You[\s\n]+are[\s\n]+accessing[\s\n]+a[\s\n]+U\.S\.[\s\n]+Government[\s\n]+information[\s\n]+system\,[\s\n]+which[\s\n]+includes:[\s\n]\(1\)this[\s\n]+computer;[\s\n]\(2\)this[\s\n]+computer[\s\n]+network;[\s\n]\(3\)all[\s\n]+computers[\s\n]+connected[\s\n]+to[\s\n]+this[\s\n]+network[\s\n]+including[\s\n]+end[\s\n]+user[\s\n]+systems;[\s\n]\(4\)all[\s\n]+devices[\s\n]+and[\s\n]+storage[\s\n]+media[\s\n]+attached[\s\n]+to[\s\n]+this[\s\n]+network[\s\n]+or[\s\n]+to[\s\n]+any[\s\n]+computer[\s\n]+on[\s\n]+this[\s\n]+network;[\s\n]+and[\s\n]\(5\)[\s\n]+cloud[\s\n]+and[\s\n]+remote[\s\n]+information[\s\n]+services\.[\s\n]+This[\s\n]+information[\s\n]+system[\s\n]+is[\s\n]+provided[\s\n]+for[\s\n]+U\.S\.[\s\n]+Government- authorized[\s\n]+use[\s\n]+only\.[\s\n]+You[\s\n]+have[\s\n]+no[\s\n]+reasonable[\s\n]+expectation[\s\n]+of[\s\n]+privacy[\s\n]+regarding[\s\n]+any[\s\n]+communication[\s\n]+transmitted[\s\n]+through[\s\n]+or[\s\n]+data[\s\n]+stored[\s\n]+on[\s\n]+this[\s\n]+information[\s\n]+system\.[\s\n]+At[\s\n]+any[\s\n]+time\,[\s\n]+and[\s\n]+for[\s\n]+any[\s\n]+lawful[\s\n]+purpose\,[\s\n]+the[\s\n]+U\.S\.[\s\n]+Government[\s\n]+may[\s\n]+monitor\,[\s\n]+intercept\,[\s\n]+search\,[\s\n]+and[\s\n]+seize[\s\n]+any[\s\n]+communication[\s\n]+or[\s\n]+data[\s\n]+transiting\,[\s\n]+stored[\s\n]+on\,[\s\n]+or[\s\n]+traveling[\s\n]+to[\s\n]+or[\s\n]+from[\s\n]+this[\s\n]+information[\s\n]+system\.[\s\n]+You[\s\n]+are[\s\n]+NOT[\s\n]+authorized[\s\n]+to[\s\n]+process[\s\n]+classified[\s\n]+information[\s\n]+on[\s\n]+this[\s\n]+information[\s\n]+system\.[\s\n]+Unauthorized[\s\n]+or[\s\n]+improper[\s\n]+use[\s\n]+of[\s\n]+this[\s\n]+system[\s\n]+may[\s\n]+result[\s\n]+in[\s\n]+suspension[\s\n]+or[\s\n]+loss[\s\n]+of[\s\n]+access[\s\n]+privileges\,[\s\n]+disciplinary[\s\n]+action\,[\s\n]+and[\s\n]+civil[\s\n]+and\/or[\s\n]+criminal[\s\n]+penalties\.

To configure the system login banner, edit `/etc/issue`. Replace the default text with current NASA accepted NASA IT System Use Notification

```
By accessing and using this information system, you acknowledge and consent to
the following:

You are accessing a U.S. Government information system, which includes: (1)
this computer; (2) this computer network; (3) all computers connected to this
network including end user systems; (4) all devices and storage media attached
to this network or to any computer on this network; and (5) cloud and remote
information services. This information system is provided for U.S.
Government-authorized use only. This system contains Controlled Unclassified
Information (CUI). You have no reasonable expectation of privacy regarding any
communication transmitted through or data stored on this information system. At
any time, and for any lawful purpose, the U.S. Government may monitor,
intercept, search, and seize any communication or data transiting, stored on,
or traveling to or from this information system. You are NOT authorized to
process classified information on this information system. Unauthorized or
improper use of this system may result in suspension or loss of access
privileges, disciplinary action, and civil and/or criminal penalties.
```

The banner file can be modified to different locations, the default being `/etc/issue`. Modification on some system (RHEL) can be done in `login.defs` as well as PAM files using `pam_issue`. For Ubuntu systems, only `pam_issue` modifies the location of the banner file.

For Suse Linux Enterprise 15, the use of the `issue-generator` and a symbolic link to `/run/issue` for `/etc/issue` builds the file from `/usr/lib/issue.d/` and `/etc/issue.d/` files. Placing the banner text into the `/etc/issue.d/99-`

NASA file will result in the banner displayed after the default system information. Suse Linux Enterprise 15 also honors both login.defs and pam_issue.

Rationale

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

bash fix

```
if [ -L /etc/issue ]
then
  fold -s > /etc/issue.d/99-NASA << EOF
By accessing and using this information system, you acknowledge and consent to the following:

You are accessing a U.S. Government information system, which includes: (1) this computer; (2) this computer network; (3) all computers connected to this network including end user systems; (4) all devices and storage media attached to this network or to any computer on this network; and (5) cloud and remote information services. This information system is provided for U.S. Government-authorized use only. This system contains Controlled Unclassified Information (CUI). You have no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system. At any time, and for any lawful purpose, the U.S. Government may monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from this information system. You are NOT authorized to process classified information on this information system. Unauthorized or improper use of this system may result in suspension or loss of access privileges, disciplinary action, and civil and/or criminal penalties.
EOF
else
fold -s > /etc/issue << EOF
By accessing and using this information system, you acknowledge and consent to the following:

You are accessing a U.S. Government information system, which includes: (1) this computer; (2) this computer network; (3) all computers connected to this network including end user systems; (4) all devices and storage media attached to this network or to any computer on this network; and (5) cloud and remote information services. This information system is provided for U.S. Government-authorized use only. This system contains Controlled Unclassified Information (CUI). You have no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system. At any time, and for any lawful purpose, the U.S. Government may monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from this information system. You are NOT authorized to process classified information on this information system. Unauthorized or improper use of this system may result in suspension or loss of access privileges, disciplinary action, and civil and/or criminal penalties.
EOF
fi
```

NASA-ASCS-20037: Enable Auditing for Processes Which Start Prior to the Audit Daemon

NASA ASCS ID	NASA-ASCS-20037
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-14 (1)
STIG Reference	RHEL_8_STIG RHEL-08-030601
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.1.3
MITRE ATT&CK Reference	T1562.001
MITRE D3FEND Reference	D3-PH

To ensure all processes can be audited, even those which start prior to the audit daemon, add the argument `audit=1` to the default GRUB 2 command line for the Linux operating system in `/etc/default/grub` in the manner below:

```
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=VolGroup/LogVol06 rd.lvm.lv=VolGroup/lv_swap rhgb
quiet rd.shell=0 audit=1"
```

Additional information on kernel parameters can be found here: https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html

Additional information on grub configuration can be found here: https://www.gnu.org/software/grub/manual/grub/html_node/Simple-configuration.html#Simple-configuration

Rationale

Each process on the system carries an auditable flag that indicates whether its activities can be audited. Although auditd takes care of enabling this for all processes which launch after it does, adding the kernel argument ensures it is set for every process during boot.

bash fix

```
if grep -Eq "^GRUB_CMDLINE_LINUX(_DEFAULT)?=" /etc/default/grub
then
  if grep -Eq "^GRUB_CMDLINE_LINUX(_DEFAULT)?=.*\baudit\b=" /etc/default/grub
  then
    sed -i "s/\s*\baudit\b=.\s*/ /g" /etc/default/grub
    sed -i "s/^GRUB_CMDLINE_LINUX=\"\(.*\)\?\"/GRUB_CMDLINE_LINUX=\"\1 audit=1\"/"
/etc/default/grub
  else
    sed -i "s/^GRUB_CMDLINE_LINUX=\"\(.*\)\?\"/GRUB_CMDLINE_LINUX=\"\1 audit=1\"/"
/etc/default/grub
  fi
else
```

```
  echo "GRUB_CMDLINE_LINUX=\"audit=1\"" >> /etc/default/grub
fi

if which rpm &> /dev/null
then
  for GRUBCFG in $( find /boot -name grub.cfg )
  do
    grub2-mkconfig -o $GRUBCFG
  done
elif which dpkg &> /dev/null
then
  update-grub
else
  echo "could not determine configuration"
fi
```

NASA-ASCS-20045: Verify grub.cfg Group Ownership

NASA ASCS ID	NASA-ASCS-20045
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	M1022, T1547
MITRE D3FEND Reference	D3-LFP

All boot configurations in the `/boot` directory named `grub.cfg` need to be group-owned by the `root` group to prevent destruction or modification of the file. To properly set the group owner of `grub.cfg` , run the command:

```
find /boot -name grub.cfg -exec chgrp root '{}' \;
```

Rationale

The root group is a highly-privileged group. Furthermore, the group-owner of this file should not have any access privileges anyway.

bash fix

```
find /boot \( -name grub.cfg -o -name grub.conf \) -exec chgrp root '{}' \;
```

NASA-ASCS-20046: Verify Group Who Owns group File

NASA ASCS ID	NASA-ASCS-20046
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the group owner of `/etc/group` , run the command:

```
$ chgrp root /etc/group
```

Rationale

The /etc/group file contains information regarding groups that are configured on the system. Protection of this file is important for system security.

bash fix

```
chgrp root /etc/group
```

NASA-ASCS-20047: Verify Group Who Owns gshadow File

NASA ASCS ID	NASA-ASCS-20047
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the group owner of `/etc/gshadow` , run the command:

For Red Hat based systems

```
chgrp root /etc/gshadow
```

For Ubuntu based systems

```
chgrp shadow /etc/gshdaow
```

Rationale

The /etc/gshadow file contains group password hashes. Protection of this file is critical for system security.

bash fix

```
if ! [ -f /etc/gshadow ]
then
  touch /etc/gshadow
fi
if [[ "$OS_LIKE" == "fedora" ]]
then
  chgrp root /etc/gshadow
elif [[ "$OS_LIKE" == "debian" ]]
then
  chgrp shadow /etc/gshadow
fi
```

NASA-ASCS-20048: Verify Group Who Owns passwd File

NASA ASCS ID	NASA-ASCS-20048
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
STIG Reference	RHEL_8_STIG RHEL-08-010740
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the group owner of `/etc/passwd` , run the command:

```
$ chgrp root /etc/passwd
```

Rationale

The /etc/passwd file contains information about the users that are configured on the system. Protection of this file is critical for system security.

bash fix

```
chgrp root /etc/passwd
```

NASA-ASCS-20049: Verify User Who Owns group File

NASA ASCS ID	NASA-ASCS-20049
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the owner of `/etc/group` , run the command:

```
$ chown root /etc/group
```

Rationale

The /etc/group file contains information regarding groups that are configured on the system. Protection of this file is important for system security.

bash fix

```
chown root /etc/group
```

NASA-ASCS-20050: Verify User Who Owns gshadow File

NASA ASCS ID	NASA-ASCS-20050
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the owner of `/etc/gshadow` , run the command:

```
$ chown root /etc/gshadow
```

Rationale

The /etc/gshadow file contains group password hashes. Protection of this file is critical for system security.

bash fix

```
if ! [ -f /etc/gshadow ]
then
  touch /etc/gshadow
fi
chown root /etc/gshadow
```

NASA-ASCS-20051: Verify User Who Owns passwd File

NASA ASCS ID	NASA-ASCS-20051
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the owner of `/etc/passwd` , run the command:

```
$ chown root /etc/passwd
```

Rationale

The /etc/passwd file contains information about the users that are configured on the system. Protection of this file is critical for system security.

bash fix

```
chown root /etc/passwd
```

NASA-ASCS-20052: Verify Permissions on group File

NASA ASCS ID	NASA-ASCS-20052
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.1.5
MITRE ATT&CK Reference	T1548, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the permissions of `/etc/group` , run the command:

```
$ chmod 644 /etc/group
```

Rationale

The /etc/group file contains information regarding groups that are configured on the system. Protection of this file is important for system security.

bash fix

```
chmod 0644 /etc/group
```

NASA-ASCS-20053: Verify Permissions on gshadow File

NASA ASCS ID	NASA-ASCS-20053
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.1.6
MITRE ATT&CK Reference	T1547, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the permissions of `/etc/gshadow` , run the command:

```
$ chmod 0000 /etc/gshadow
```

Rationale

The /etc/gshadow file contains group password hashes. Protection of this file is critical for system security.

bash fix

```
if ! [ -f /etc/gshadow ]
then
  touch /etc/gshadow
fi
chmod 0000 /etc/gshadow
```

NASA-ASCS-20054: Verify Permissions on passwd File

NASA ASCS ID	NASA-ASCS-20054
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
STIG Reference	RHEL_8_STIG RHEL-08-010730
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.1.3
MITRE ATT&CK Reference	T1547, M1022
MITRE D3FEND Reference	D3-LFP, D3-CSP

To properly set the permissions of `/etc/passwd` , run the command:

```
$ chmod 0644 /etc/passwd
```

Rationale

If the /etc/passwd file is writable by a group-owner or the world, the risk of its compromise is increased. The file contains a list of accounts on the system with associated information. As such, the protection of this file is critical to support system security.

bash fix

```
chmod 0644 /etc/passwd
```

NASA-ASCS-20055: Verify Permissions on shadow File

NASA ASCS ID	NASA-ASCS-20055
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.1.4
MITRE ATT&CK Reference	M1022, T1547
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the permissions of `/etc/shadow` , run the command:

```
$ chmod 0000 /etc/shadow
```

Rationale

The `/etc/shadow` file contains the list of local system accounts and stores password hashes. Protection of this file is critical for system security. Failure to have proper permissions of this file provides unintended access to sensitive information, which could weaken the system security posture.

bash fix

```
chmod 0000 /etc/shadow
```

NASA-ASCS-20056: Verify grub.cfg Permissions

NASA ASCS ID	NASA-ASCS-20056
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	M1022, T1547
MITRE D3FEND Reference	D3-LFP

File permissions for grub configuration should be unaltered from what is set by the operating system during the grub configuration file build process.

Depending on the configuration and distribution the permissions set can range from 700 to 664. In all cases it is

crucial that the permissions of `grub.cfg` or `grub.conf` file do not allow anyone but `root` to write to it.

Rebuilding the `grub` configuration file using the `grub2-mkconfig` in Red Hat based systems and the `update-grub` utility on Debian based systems.

Finding if all files in the system are disallowing write by other can be done with this command:

```
find /boot \( -name grub.cfg -o -name grub2.cfg -o -name grub.conf \) -perm -o+w
```

Rationale

Proper permissions ensure that only the root user can modify important boot parameters.

bash fix

```
find /boot \( -name grub.cfg -o -name grub2.cfg -o -name grub.conf \) -perm -o+w -exec chmod o-w
'{}' \;
```

NASA-ASCS-20057: Verify grub.cfg User Ownership

NASA ASCS ID	NASA-ASCS-20057
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	M1022, T1547
MITRE D3FEND Reference	D3-LFP

The grub configuration file should be owned by the `root` user to prevent destruction or modification of the file. To properly set the owner of `grub.cfg` or `grub.conf` file, run the command:

```
$ find /boot -name grub.cfg -o -name grub.conf -exec chown root '{}' \;
```

Rationale

Only root should be able to modify important boot parameters.

bash fix

```
find /boot -name grub.cfg -exec chown root '{}' \;
```

NASA-ASCS-20083: Uninstall rsh Package

NASA ASCS ID	NASA-ASCS-20083
Severity	**High**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-040010
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 2.3.2
MITRE ATT&CK Reference	TA0006, TA0008, M1042

The `rsh` package contains the client commands for the rsh services and shall be removed. Packages can be removed with the following command:

```
yum remove rsh
```

or

```
apt-get purge rsh-client
```

Rationale

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and thereby expose their credentials. Note that removing the rsh package removes the clients for rsh, rcp, and rlogin.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q rsh &> /dev/null
  then
    yum -y remove rsh &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' rsh-client )" == "installed" ]]
  then
    apt-get -y purge rsh-client &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q rsh &> /dev/null
  then
    zypper --non-interactive remove rsh &> /dev/null
  fi
fi
```

NASA-ASCS-20084: Ensure rsyslog is Installed

NASA ASCS ID	NASA-ASCS-20084
Severity	**High**
Group	logging/system
STIG Reference	RHEL_8_STIG RHEL-08-030670
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 4.2.1.2
MITRE D3FEND Reference	D3-OSM

The `rsyslog` package is the default system level logging facility in Linux.

The `rsyslog` package shall be installed with the following command:

```
yum install rsyslog
```

or

```
apt-get install rsyslog
```

or

```
zypper install rsyslog
```

Rationale

The rsyslog package provides the rsyslog daemon, which provides system logging services.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if ! rpm -q rsyslog &> /dev/null
  then
    yum -y install rsyslog &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' rsyslog )" != "installed" ]]
  then
    apt-get -y install rsyslog &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
```

```
  if ! rpm -q rsyslog &> /dev/null
  then
    zypper --non-interactive install rsyslog &> /dev/null
  fi
fi
```

NASA-ASCS-20085: Remove telnet Clients

NASA ASCS ID	NASA-ASCS-20085
Severity	**High**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-040000
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 2.3.4
MITRE ATT&CK Reference	TA0006, T1557, T1036, M1042

The telnet client allows users to start connections to other systems via the telnet protocol.

The telnet client has been deemed insecure by most security practices. While telnet as a utility can be used for other actions beyond use of the telnet protocol, many other tools can provide the same function without the overhead of an insecure software. The use of the netcat tool (`nc`) can perform the same connection analysis as the telnet client.

Remove `telnet` package with the following command:

```
yum remove telnet
```

or

```
apt-get purge telnet
```

or

```
zypper remove telnet
```

Rationale

The telnet protocol is neither secure nor encrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
```

```
then
  if rpm -q telnet &> /dev/null
  then
    yum -y remove telnet &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' telnet )" == "installed" ]]
  then
    apt-get -y purge telnet &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q telnet &> /dev/null
  then
    zypper --non-interactive remove telnet &> /dev/null
  fi
fi
```

NASA-ASCS-20093: Ensure Log Files Are Owned By Appropriate Group

NASA ASCS ID	NASA-ASCS-20093
Severity	**High**
Group	logging/system
NIST SP 800-53r5 Reference	AU-09
MITRE ATT&CK Reference	T1070.002, M1029, M1022
MITRE D3FEND Reference	D3-LFP

The group-owner of all log files written by `rsyslog` need to be maintained to prevent inappropriate alteration. The group-owner is designated in the `/etc/rsyslog.conf` using the global directive `$FileGroup` value. The global directive can be changed for each log file entry.

Due to the complexity of rsyslog and the capacity it has to be configured in an insecure way, groups are acceptable `$FileGroup` value as the default `root`, or group value that exist with a service account gid (under 1000). From the perspective of monitoring, the allowed groups will be checked on files denoted in the `/etc/rsyslog.conf` and included files.

For each log file `LOGFILE` referenced in `/etc/rsyslog.conf`, run the following command to inspect the file's group-owner:

```
$ stat -c %G LOGFILE
```

If the group-owner is not the same as detailed in the global directive `$FileGroup` preceding the file name of the configuration file, run the following command to correct this:

```
$ chgrp <FileGroup> LOGFILE
```

Rationale

The log files generated by rsyslog contain valuable information regarding system configuration, user authentication, and other such information. Log files should be protected from unauthorized access.

bash fix

```
RSYSLOG_FILES=$(grep -v "^[\$#]" /etc/rsyslog.{conf,d/*} 2> /dev/null | grep -E -- "\s+-?\/" | sed
"s/^.*\s\-\?\(\/.*\)/\1/" | grep -vE "(\/\*|\/dev)")
for FILE in $RSYSLOG_FILES
do
  if [ -e $FILE ]
  then
    if [[ "$( stat -c '%g' $FILE )" -ge 1000 ]]
    then
      echo "$FILE needs to be changed manually to gid of a service account. "
    fi
  fi
done
```

NASA-ASCS-20094: Ensure Log Files Are Owned By Appropriate User

NASA ASCS ID	NASA-ASCS-20094
Severity	**High**
Group	logging/system
NIST SP 800-53r5 Reference	AU-09
MITRE ATT&CK Reference	T1070.002, M1029, M1022
MITRE D3FEND Reference	D3-LFP

The owner of all log files written by `rsyslog` need to be maintained to prevent inappropriate alteration. The owner is designated in the `/etc/rsyslog.conf` using the global directive `$FileOwner` value. The global directive can be changed for each log file entry.

Due to the complexity of rsyslog and the capacity it has to be configured in an insecure way, groups are acceptable `$FileOwner` value as the default `root`, or user id value that exist with a service account uid (under 1000). From the perspective of monitoring, the allowed groups will be checked on files denoted in the `/etc/rsyslog.conf` and included files.

For each log file `LOGFILE` referenced in `/etc/rsyslog.conf`, run the following command to inspect the file's owner:

```
$ stat -c %U LOGFILE
```

If the owner is not the same as detailed in the global directive `$FileOwner` preceding the file name of the configuration file, run the following command to correct this:

```
$ chown <FileOwner> LOGFILE
```

Rationale

The log files generated by rsyslog contain valuable information regarding system configuration, user authentication, and other such information. Log files should be protected from unauthorized access.

bash fix

```
RSYSLOG_FILES=$(grep -v "^[\$#]" /etc/rsyslog.{conf,d/*} 2> /dev/null | grep -E -- "\s+-?\/" | sed
"s/^.*\s\-\?\(\/.*\)/\1/" | grep -vE "(\/\*|\/dev)")
for FILE in $RSYSLOG_FILES
do
  if [ -e $FILE ]
  then
    if [[ "$( stat -c '%u' $FILE )" -ge 1000 ]]
    then
      echo "$FILE needs to be changed manually to uid of a service account. "
    fi
  fi
done
```

NASA-ASCS-20095: Ensure System Log Files Have Correct Permissions

NASA ASCS ID	NASA-ASCS-20095
Severity	**High**
Group	logging/system
NIST SP 800-53r5 Reference	AU-09, AC-03 (4)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 4.2.1.4
MITRE ATT&CK Reference	T1070.002, M1029, M1022
MITRE D3FEND Reference	D3-LFP

The file permissions for all log files written by `rsyslog` need to be set appropriately. The `/etc/rsyslog.conf` file specify the `$FileCreateMode` and `$umask` global directives. The global directive can be changed for each log file

entry.

Due to the complexity of rsyslog and the capacity it has to be configured in an insecure way, files designated by the `/etc/rsyslog.conf` and included `/etc/rsyslog.d/` files need to be set to a maximum permission value of `0640`.

For each log file `LOGFILE` referenced in the configuration, run the following command to inspect the file's permissions:

```
$ stat -c %G LOGFILE
```

If the group-owner is not the same as detailed in the global directive `$FileGroup` preceding the file name of the configuration file, run the following command to correct this:

```
$ chgrp <FileGroup> LOGFILE
```

```
stat -c %a LOGFILE
```

If the permissions are not 640, run the following command to correct this:

```
chmod 0640 LOGFILE
```

Rationale

Log files can contain valuable information regarding system configuration. If the system log files are not protected, unauthorized users could change the logged data, eliminating their forensic value.

bash fix

```
RSYSLOG_FILES=$(grep -Ev "^(\s+)?[\$#]" /etc/rsyslog.{conf,d/*} 2> /dev/null | grep -E -- "\s+-?\/"
| sed "s/^.*\s\-\?\(\/.*\)/\1/" | grep -vE "(\/\*|\/dev)")
for FILE in $RSYSLOG_FILES
do
  if [ -e $FILE ]
  then
    if ! stat -c "%A" $FILE | grep -E -- "-r[w-]-[r-]-----" &> /dev/null
    then
      echo "$FILE needs to be changed manually -rw-r-----"
    fi
  fi
done
```

NASA-ASCS-20103: Enable rsyslog Service

NASA ASCS ID	NASA-ASCS-20103

Severity	**High**
Group	logging/system
STIG Reference	RHEL_8_STIG RHEL-08-010561
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 4.2.1.2
MITRE ATT&CK Reference	M1029
MITRE D3FEND Reference	D3-OSM

The `rsyslog` service provides syslog-style logging. The `rsyslog` service shall be enabled with the following command:

```
$ systemctl enable rsyslog.service
```

or

```
chkconfig rsyslog on
```

Rationale

The rsyslog service must be running in order to provide logging services, which are essential to system administration.

bash fix

```
if which systemctl &> /dev/null
then
  SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?(r)?syslog(d)?\.service" | sed "s/^\s\+//"
| cut -d" " -f1 )
  systemctl enable $SERVICE &> /dev/null
  systemctl start $SERVICE &> /dev/null
else
  SERVICE=$( chkconfig | grep -E "^(\s+)?(r)?syslog" | cut -d" " -f1 )
  chkconfig $SERVICE on &> /dev/null
  service $SERVICE start &> /dev/null
fi
```

NASA-ASCS-20109: Enable Randomized Layout of Virtual Address Space

NASA ASCS ID	NASA-ASCS-20109
Severity	**High**
Group	permissions/system

NIST SP 800-53r5 Reference	SI-16
STIG Reference	RHEL_8_STIG RHEL-08-010430
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.5.3
MITRE ATT&CK Reference	T1055, M1026
Control Setting	2

To set the runtime status of the `kernel.randomize_va_space` kernel parameter, run the following command:

```
$ sysctl -w kernel.randomize_va_space=2
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
kernel.randomize_va_space = 2
```

Rationale

Address Space Layout Randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code they have introduced into a processs address space during an attempt at exploitation. Additionally, ASLR makes it more difficult for an attacker to know the location of existing code in order to repurpose it using Return Oriented Programming (ROP) techniques.

bash fix

```
CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^kernel.randomize_va_space"
SED_INLINE="s/^kernel.randomize_va_space.*$/kernel.randomize_va_space=2/"
ECHO_APPEND="kernel.randomize_va_space=2"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20118: Set Daemon Umask

NASA ASCS ID	NASA-ASCS-20118
Severity	**High**
Group	permissions/system

MITRE D3FEND Reference	D3-LFP
Control Setting	022

The file `/etc/init.d/functions` includes initialization parameters for most or all daemons started at boot time. The default umask of 022 prevents creation of group- or world-writable files. To set the default umask for daemons, edit the following line:

```
umask  022
```

Setting the umask to too restrictive a setting can cause serious errors at runtime. Many daemons on the system already individually restrict themselves to a umask of 077 in their own init scripts.

if file `/etc/init.d/functions` does not exist, the check will be considered a pass, since SysV support is considered disabled.

Rationale

The umask influences the permissions assigned to files created by a process at run time. An unnecessarily permissive umask could result in files being created with insecure permissions.

bash fix

```
if [ -e /etc/init.d/functions ]
then
  if grep -qE "^(\s*)?umask" /etc/init.d/functions
  then
    sed -i "s/umask.*/umask 022/g" /etc/init.d/functions
  else
    echo "umask 022" >> /etc/init.d/functions
  fi
fi
```

NASA-ASCS-20119: Verify User Who Owns shadow File

NASA ASCS ID	NASA-ASCS-20119
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
MITRE ATT&CK Reference	T1547, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the owner of `/etc/shadow` , run the command:

```
$ chown root /etc/shadow
```

Rationale

The /etc/shadow file contains the list of local system accounts and stores password hashes. Protection of this file is critical for system security. Failure to give ownership of this file to root provides the designated owner with access to sensitive information which could weaken the system security posture.

bash fix

```
chown root /etc/shadow
```

NASA-ASCS-20126: Set Password Retry Prompts Permitted Per-Session

NASA ASCS ID	NASA-ASCS-20126
Severity	**High**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-020100, RHEL_8_STIG RHEL-08-020102, RHEL_8_STIG RHEL-08-020103, RHEL_8_STIG RHEL-08-020104
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.5.1
MITRE ATT&CK Reference	T1110, M1027
Control Setting	5

Set the `pwquality retry` value to 5 or lower.

This can be accomplished using the `/etc/security/pwquality.conf` entry or the `pam_pwquality` pam line directly in the `/etc/pam.d` configurations. **It is recommended to use the `/etc/security/pwquality.conf` file over inline `/etc/pam.d/` configuration.**

Ubuntu 18.04 does not honor the retry value for `/etc/securuty/pwquality.conf` setting, it is advised to place in both file and pam configurations.

If using the `/etc/security/pwquality.conf` file for this control, use it also on control 20003 (minlen), do not mix it with using cracklib or pam_pwquality in the pam files.

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-update`. Refer to distribution documentation for appropriate configuration use. The PIV-SSSD Handbook has both `authselect` and `pam-auth-update` content that can also help.

Maintaining password quality on systems is to ensure that whenever a user becomes PIV exempt, they can still access the system. PIV exempt users should always be unable to elevate privileges unless other controls are in place.

System Owners that would prefer to have more restriction for password abuse on systems, such as high security systems, should also consider configuration of `pam_faillock.so` in order to implement account lockout when numerous attempts to authenticate are reached. However, be aware that locking out user accounts presents the risk of a denial-of-service attack. The lockout policy must weigh whether the risk of such a denial-of-service attack outweighs the benefits of thwarting password guessing attacks.

Rationale

Setting the password retry prompts that are permitted on a per-session basis to a low value requires some software, such as SSH, to reconnect. This can slow down and draw additional attention to some types of password-guessing attacks. Note that this is different from account lockout, which is provided by the pam_faillock module.

bash fix

```
if [ -f /etc/security/pwquality.conf ]
then
  VAL=$(grep -E "^(\s+)?retry" /etc/security/pwquality.conf | sed -e "s/\s\+//g" | cut -d= -f2)
  if ! [ $VAL ]
  then
    echo "retry = 5" >> /etc/security/pwquality.conf
  elif [[ "$VAL" -gt "5" ]]
  then
    sed -i "s/^retry.*$/retry\ =\ 5/" /etc/security/pwquality.conf
  fi
else
  echo "Remediation only considers /etc/security/pwquality.conf used in modern linux versions."
fi
```

NASA-ASCS-20129: Record Events that Modify the System Discretionary Access Controls (DAC) - chmod

NASA ASCS ID	NASA-ASCS-20129
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030490
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047

MITRE D3FEND Reference	D3-OSM

Monitor all events using `chmod`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="chmod"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "(\s+)?#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20130: Record Events that Modify the System Discretionary Access Controls (DAC) - chown

NASA ASCS ID	NASA-ASCS-20130
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)

STIG Reference	RHEL_8_STIG RHEL-08-030480, RHEL_8_STIG RHEL-08-030100
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `chown`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="chown"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20131: Record Events that Modify the System Discretionary Access Controls (DAC) - fchmod

NASA ASCS ID	NASA-ASCS-20131

Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030490
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `fchmod`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="fchmod"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20132: Record Events that Modify the System Discretionary Access Controls (DAC) - fchmodat

NASA ASCS ID	NASA-ASCS-20132
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030490
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `fchmodat`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="fchmodat"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
```

```
done
```

NASA-ASCS-20133: Record Events that Modify the System Discretionary Access Controls (DAC) - fchown

NASA ASCS ID	NASA-ASCS-20133
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030480
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `fchown`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="fchown"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
```

```
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20134: Record Events that Modify the System Discretionary Access Controls (DAC) - fchownat

NASA ASCS ID	NASA-ASCS-20134
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030480
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `fchownat`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="fchownat"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20135: Record Events that Modify the System Discretionary Access Controls (DAC) - fremovexattr

NASA ASCS ID	NASA-ASCS-20135
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `fremovexattr`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="fremovexattr"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20136: Record Events that Modify the System Discretionary Access Controls (DAC) - fsetxattr

NASA ASCS ID	NASA-ASCS-20136
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D4-OSM

Monitor all events using `fsetxattr`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="fsetxattr"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20137: Record Events that Modify the System Discretionary Access Controls (DAC) - lchown

NASA ASCS ID	NASA-ASCS-20137
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030480
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `lchown`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

```
-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="lchown"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20138: Record Events that Modify the System Discretionary Access Controls (DAC) - lremovexattr

NASA ASCS ID	NASA-ASCS-20138
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `lremovexattr`.

The auditd daemon is configured to use the augenrules program to read audit rules during daemon startup (the default), add the following lines to a file with suffix .rules in the directory /etc/audit/rules.d, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The auid value shown as 4294967295 may appear on inspection of the control as either -1 or unset, this is a valid return and all the values have the same meaning to auditd.

The -F key= or -k flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="lremovexattr"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20139: Record Events that Modify the System Discretionary Access Controls (DAC) - lsetxattr

NASA ASCS ID	NASA-ASCS-20139
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047

MITRE D3FEND Reference	D3-OSM

Monitor all events using `lsetxattr`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="lsetxattr"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20140: Record Events that Modify the System Discretionary Access Controls (DAC) - removexattr

NASA ASCS ID	NASA-ASCS-20140
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)

STIG Reference	RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `chmod`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="removexattr"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20141: Record Events that Modify the System Discretionary Access Controls (DAC) - setxattr

NASA ASCS ID	NASA-ASCS-20141

Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030200
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.9
MITRE ATT&CK Reference	TA0005, T1222, M1047
MITRE D3FEND Reference	D3-OSM

Monitor all events using `setxattr`.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`, setting for both b32 and b64:

```
-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod
```

The `auid` value shown as `4294967295` may appear on inspection of the control as either `-1` or `unset`, this is a valid return and all the values have the same meaning to `auditd`.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

bash fix

```
CONTROL="setxattr"
for ARCH in b32 b64
do
  if ! [[ "$( grep -Ev "^\s*#" /etc/audit/rules.d/* | grep -E -- "-S\s([a-zA-Z0-9,_-
]*)?\b$CONTROL\b(,)?" | grep -E -- "-F\sarch=$ARCH(\s|$)" )" ]]
  then
    echo "-a always,exit -F arch=$ARCH -S $CONTROL -F auid>=1000 -F auid!=4294967295 -F
key=perm_mod" >> /etc/audit/rules.d/35-dac_controls.rules
  fi
done
```

NASA-ASCS-20143: Ensure auditd Collects Information on the Use of Privileged Commands

NASA ASCS ID	NASA-ASCS-20143
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030190, RHEL_8_STIG RHEL-08-030250, RHEL_8_STIG RHEL-08-030280, RHEL_8_STIG RHEL-08-030290, RHEL_8_STIG RHEL-08-030300, RHEL_8_STIG RHEL-08-030301, RHEL_8_STIG RHEL-08-030310, RHEL_8_STIG RHEL-08-030311, RHEL_8_STIG RHEL-08-030312, RHEL_8_STIG RHEL-08-030313, RHEL_8_STIG RHEL-08-030314, RHEL_8_STIG RHEL-08-030315, RHEL_8_STIG RHEL-08-030316, RHEL_8_STIG RHEL-08-030317, RHEL_8_STIG RHEL-08-030320, RHEL_8_STIG RHEL-08-030340, RHEL_8_STIG RHEL-08-030370, RHEL_8_STIG RHEL-08-030400, RHEL_8_STIG RHEL-08-030560
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.6
MITRE ATT&CK Reference	TA0002, T1059, M1026, TA0004, T1548, M1047
MITRE D3FEND Reference	D3-OSM

At a minimum, the audit system should collect the execution of privileged commands for all users and root. To find the relevant setuid / setgid programs, run the following command for each local partition PART:

```
$ find PART -type f \( -perm -4000 -o -type f -perm -2000 \) 2>/dev/null
```

Structures can also be excluded in the search

```
$ find PART -not -path /var/lib/docker/* -type f \( -perm -4000 -o -type f -perm -2000 \)
2>/dev/null
```

Mounts with the `noexec` and `nosuid` flag will be excluded since the system will not allow execution from these mount points. (Addition of `nosuid` changed in the FY2023 R4 release)

It is still possible to execute scripting code that bypasses the `nosuid` and the `noexec` flag since the script execution element may not be on an executable volume.

During CDM checking we have found that large filesystems with MacOS and Windows files in them will cause processor spikes and processes to hang during the execution of this control check. In order to exclude a mount point that contains large amounts of files from being checked, set the mount point with the `noexec` flag.

If the `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add a line of the following form to a file with suffix `.rules` in the directory `/etc/audit/rules.d` for each

setuid / setgid program on the system, replacing the SETUID_PROG_PATH part with the full path of that setuid / setgid program in the list:

```
-a always,exit -F path=SETUID_PROG_PATH -F perm=x -F auid>=1000 -F auid!=4294967295 -F
key=privileged_commands
```

Finding additional local partitions can be done with:

```
df -l -t xfs -t ext4 -t ext3 --output=target | tail -n +2
# Or for older instances:
df -P -l -t xfs -t ext4 -t ext3 | tail -n +2 | awk '{print $6}'
```

The auid value shown as 4294967295 may appear on inspection of the control as either -1 or unset, this is a valid return and all the values have the same meaning to auditd.

The -F key= or -k flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

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

bash fix

```
# NOTE: adding a file to the execution directory called path.exclude will allow an admin
#       to provide a list of locations, each on a single line, to be excluded from the
#       find command that will execute the privileged_commands entry into audit rules.
#       This feature is only for the remediation bash script.
FILTER=""
TIMEOUT=10m
if [ -e path.exclude ]
then
  for LINE in $(<path.exclude)
  do
    FILTER=$FILTER"-path $LINE -o "
  done
  FILTER="${FILTER:0:(-4)} -prune -o"
fi
for DEVTYPE in $( grep -v nodev /proc/filesystems | grep -vE "(fuseblk|squashfs)" )
do
  for MNTPNT in $( findmnt -ln -t $DEVTYPE -O nonoexec,nonosuid -o TARGET )
  do
    IFS_BKP="$IFS"
    IFS=$'\n'
    for FPATH in $(timeout $TIMEOUT find $MNTPNT $FILTER -xdev -not -path /var/lib/docker/* -type f
\( -perm -4000 -o -perm -2000 \) 2>/dev/null)
    do
```

```
      if ! [[ "$( grep -E -- "-F\s+path=$( echo $FPATH | sed "s/\//\\\\\//g" )"
/etc/audit/rules.d/* )" ]]
      then
        echo "-a always,exit -F path=$FPATH -F perm=x -F auid>=1000 -F auid!=4294967295 -F
key=privileged_commands" >> /etc/audit/rules.d/21-priv_commands.rules
      fi
    done
    IFS="$IFS_BKP"
  done
done
```

NASA-ASCS-20144: Ensure auditd Collects System Administrator Access Changes

NASA ASCS ID	NASA-ASCS-20144
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030171, RHEL_8_STIG RHEL-08-030172
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.3
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM

Monitor changes to configurations providing access to elevate privileges as a system administrator.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`:

```
-w /etc/sudoers -p wa -F key=sysadmin_actions
-w /etc/sudoers.d/ -p wa -F key=sysadmin_actions
```

The `sudo` command, and other privileged commands, are tracked in NASA-ASCS-20143.

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

Rationale

The actions taken by system administrators are audited to keep a record of what was executed on the system for the purpose of providing accountability.

bash fix

```
if [ ! "$( grep -E -- "-w\s+\/etc\/sudoers(\s|$)" /etc/audit/rules.d/* )" ]
then
  echo "-w /etc/sudoers -p wa -F key=sysadmin_actions" >> /etc/audit/rules.d/20-
sysadmin_commands.rules
fi
if [ ! "$( grep -E -- "-w\s+\/etc/sudoers\.d(\s|$)" /etc/audit/rules.d/* )" ]
then
  echo "-w /etc/sudoers.d -p wa -F key=sysadmin_actions" >> /etc/audit/rules.d/20-
sysadmin_commands.rules
fi
```

NASA-ASCS-20145: Record Events that Modify User/Group Information

NASA ASCS ID	NASA-ASCS-20145
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12, AC-06 (9)
STIG Reference	RHEL_8_STIG RHEL-08-030171, RHEL_8_STIG RHEL-08-030172, RHEL_8_STIG RHEL-08-030370
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.8
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM

Monitor all changes to user and group configurations.

The `auditd` daemon is configured to use the `augenrules` program to read audit rules during daemon startup (the default), add the following lines to a file with suffix `.rules` in the directory `/etc/audit/rules.d`:

```
-w /etc/group -p wa -F key=usergroup_modification_rules
-w /etc/passwd -p wa -F key=usergroup_modification_rules
-w /etc/gshadow -p wa -F key=usergroup_modification_rules
-w /etc/shadow -p wa -F key=usergroup_modification_rules
-w /etc/security/opasswd -p wa -F key=usergroup_modification_rules
```

The `-F key=` or `-k` flags indicate the same field in the audit logging. The key field is not monitored by the compliance check as it is an arbitrary value to help an admin when filtering audit reports.

This control has a known issue with AVC alerting and messages generated in some situations. If a system is being hindered by these messages, SELinux can be quieted. The following block of commands will prevent the audit log

from being generated, without causing the SELinux from completing the blocking action.

```
cat > bigfix_quiet.te << END_OF_FILE
module bigfix_quiet 1.0;

require {
    type iptables_t;
    type sshd_t;
    type var_t;
    type initrc_t;
    type auditctl_t;
    class file write;
}

#============= auditctl_t ==============

#!!!! WARNING: 'var_t' is a base type.
dontaudit auditctl_t var_t:file write;

#============= iptables_t ==============

#!!!! WARNING: 'var_t' is a base type.
dontaudit iptables_t var_t:file write;

#============= sshd_t ==============

#!!!! WARNING: 'var_t' is a base type.
dontaudit sshd_t var_t:file write;
END_OF_FILE

checkmodule -M -m -o bigfix_quiet.mod bigfix_quiet.te
semodule_package -o bigfix_quiet.pp -m bigfix_quiet.mod
semodule -i bigfix_quiet.pp
```

Rationale

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

bash fix

```
FLIST=("/etc/group" "/etc/shadow" "/etc/passwd" "/etc/gshadow" "/etc/security/opasswd")

for FITEM in ${FLIST[*]}
do
  if [ ! "$( grep -E -- "-w\s+$FITEM" /etc/audit/rules.d/* | grep -E -- "-p\swa"  )" ]
  then
    echo "-w $FITEM -p wa -F key=usergroup_modification_rules" >> /etc/audit/rules.d/15-
usergroup_mods.rules
  fi
done
```

NASA-ASCS-20152: Specify a Remote Network Time Server

NASA ASCS ID	NASA-ASCS-20152
Severity	**High**
Group	ntp/services
NIST SP 800-53r5 Reference	SC-45 (1)
STIG Reference	RHEL_8_STIG RHEL-08-030740
MITRE ATT&CK Reference	TA0005, T1562.001
Control Setting	ntp.nasa.gov,time.nasa.gov

Depending on specific functional requirements of a concrete production environment, the system can be configured to utilize the services of the `chronyd` service, or `ntpd` NTP service.

To specify a remote network time server for synchronization, perform the following:

- if the system is configured to use `chronyd`, edit `/etc/chrony.conf`, or `/etc/chrony/chrony.conf`.
- if the system is configured to use `ntpd`, edit `/etc/ntp.conf`.

Check on setting

```
grep -E "(server|pool) [A-Za-z0-9\.\-]*\.nasa\.gov" /etc/chrony.conf # or /etc/ntp.conf
```

Rationale

Synchronizing with a remote network time server makes it possible to collate system logs from multiple sources or correlate computer events with real time events.

bash fix

```
EXISTS_IF_REGEX="^(server|pool)\s+(169\.254\.169\.123|[A-Za-z0-9\.\-]*\.nasa\.gov)"

if which systemctl &> /dev/null
then
  SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?chrony(d)?\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  SERVICE_CONF=$( find /etc -name chrony.conf )
  if [[ "$SERVICE" == "" ]]
  then
    if systemctl is-enabled systemd-timesyncd &> /dev/null
    then
      SERVICE=systemd-timesyncd.service
      SERVICE_CONF=$( find /etc/ -name timesyncd.conf )
      # reset for timesyncd
      EXISTS_IF_REGEX="^(\s+)?NTP=(169\.254\.169\.123|[A-Za-z0-9\.\-]*\.nasa\.gov)"
      SED_INLINE="s/^NTP=.*/NTP=time.nasa.gov/"
```

```
    else
      SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?ntp(d)?\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
      SERVICE_CONF=$( find /etc -name ntp.conf )
    fi
  fi
else
  SERVICE=$( chkconfig | grep -E "^(\s+)?chrony(d)?" | sed "s/^\s\+//" | cut -d" " -f1 )
  SERVICE_CONF=$( find /etc -name chrony.conf )
  if [[ "$SERVICE" == "" ]]
  then
    SERVICE=$( chkconfig | grep -E "^(\s+)?\bntp(d)?\b" | sed "s/^\s\+//" | cut -d" " -f1 )
    SERVICE_CONF=$( find /etc -name ntp.conf )
  fi
fi

if [ -e $SERVICE_CONF ]
then
  if [[ "$SERVICE" == "systemd-timesyncd.service" ]]
  then
    if grep -q "^NTP=" $SERVICE_CONF
    then
      sed -i $SED_INLINE $SERVICE_CONF
    else
      echo "NTP=time.nasa.gov" >> $SERVICE_CONF
    fi
  elif ! grep -E $EXISTS_IF_REGEX $SERVICE_CONF &> /dev/null
  then
    sed -i "s/^\(server|pool\)/#\1/" $SERVICE_CONF
    LN=$( grep -nE "^#?(server|pool)" $SERVICE_CONF | tail -n1 | cut -d: -f1 )
    head -n $LN $SERVICE_CONF > $SERVICE_CONF.tmp
    echo "pool  time.nasa.gov iburst" >> $SERVICE_CONF.tmp
    tail -n +$(( $LN + 1 )) $SERVICE_CONF >> $SERVICE_CONF.tmp
    cp -a $SERVICE_CONF $SERVICE_CONF.remediate
    cp $SERVICE_CONF.tmp $SERVICE_CONF
    rm -f $SERVICE_CONF.tmp
  fi
else
  echo "$SERVICE_CONF does not exist, manual intervention required"
fi
```

NASA-ASCS-20160: Verify that System Executables Have Restrictive Permissions

NASA ASCS ID	NASA-ASCS-20160
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)

STIG Reference	RHEL_8_STIG RHEL-08-010300
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.10
MITRE ATT&CK Reference	T1083, M1022
MITRE D3FEND Reference	D3-LFP

System executables are stored in the following directories by default:

```
/bin
/sbin
/usr/bin
/usr/libexec
/usr/local/bin
/usr/local/sbin
/usr/sbin
```

All files in these directories should not be group-writable or world-writable. If a file in these directories is found to be group-writable or world-writable, correct its permission with the following command:

```
$ chmod go-w FILE
```

Rationale

System binaries are executed by privileged users as well as system services, and restrictive permissions are necessary to ensure execution of these programs cannot be co-opted.

bash fix

```
DIRS="/bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin /usr/libexec"
for dirPath in $DIRS; do
    find "$dirPath" -perm /022 -exec chmod go-w '{}' \;
done
```

NASA-ASCS-20162: Verify All GIDs Referenced in /etc/passwd are Defined in /etc/group

NASA ASCS ID	NASA-ASCS-20162
Severity	**High**
Group	accounts/system

Add a group to the system for each GID referenced without a corresponding group.

Rationale

If a user is assigned the Group Identifier (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.

NASA-ASCS-20170: Uninstall ypserv Package

NASA ASCS ID	NASA-ASCS-20170
Severity	**High**
Group	obsolete/services
MITRE ATT&CK Reference	TA0006, T1036, TA0008, M1042

The `ypserv` package shall be removed with the following command:

```
yum remove ypserv
```

or

```
apt-get purge yp-tools nis
```

or

```
zypper remove yp-tools
```

Rationale

The Network Information Service (NIS) provides an unencrypted authentication service which does not provide for the confidentiality and integrity of user passwords or the remote session. Removing the ypserv package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q ypserv &> /dev/null
  then
    yum -y remove ypserv &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' yp-tools )" == "installed" ]]
  then
    apt-get -y purge yp-tools &> /dev/null
  fi
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' nis )" == "installed" ]]
  then
```

```
    apt-get -y purge nis &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q yp-tools &> /dev/null
  then
    zypper --non-interactive remove yp-tools &> /dev/null
  fi
fi
```

NASA-ASCS-20173: Enable auditd Service

NASA ASCS ID	NASA-ASCS-20173
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.1.2
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM

The `auditd` service is an essential userspace component of the Linux Auditing System, as it is responsible for writing audit records to disk. The `auditd` service shall be enabled with the following command:

```
$ systemctl enable auditd.service
```

or

```
chkconfig auditd on
```

Rationale

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. When the auditd service is active, it ensures audit records generated by the kernel are appropriately recorded. Additionally, a properly configured audit subsystem records actions of individual system users that can be uniquely traced to facilitate user accountability.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if ! rpm -q --quiet audit
```

```
  then
    yum -y install audit &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' auditd )" != "installed" ]]
  then
    apt-get -y install auditd &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if ! rpm -q --quiet audit
  then
    zypper --non-interactive install audit &> /dev/null
  fi
else
  echo "Could not install auditd"
fi

if which systemctl &> /dev/null
then
  SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?audit(d)?\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  if ! systemctl is-enabled $SERVICE &> /dev/null
  then
    systemctl enable $SERVICE &> /dev/null
  fi
  if ! systemctl is-active $SERVICE &> /dev/null
  then
    systemctl start $SERVICE &> /dev/null
  fi
else
  SERVICE=$( chkconfig | grep "^audit" | cut -d" " -f1 )
  chkconfig $SERVICE on &> /dev/null
  service $SERVICE start &> /dev/null
fi
```

NASA-ASCS-20175: Ensure Network Time Synchronisation is Active

NASA ASCS ID	NASA-ASCS-20175
Severity	**High**
Group	ntp/services
NIST SP 800-53r5 Reference	SC-45 (1)
MITRE ATT&CK Reference	TA0005, T1562.001

A system can synchronize its time using either `chronyd` (default) or `ntpd` (allowed only for systems that need to distribute time to peer systems).

The `chronyd` service can be enabled with the following command:

```
systemctl enable chronyd.service
systemctl start chronyd.service
```

The `ntpd` service can be enabled with the following command:

```
systemctl enable ntpd.service
systemctl start ntpd.service
```

The `systemd-timesyncd` service can be started with the following command:

```
systemctl enable systemd-timesyncd.service
systemctl start systemd-timesyncd.service
```

Rationale

Ensuring that chronyd, timesyncd, or ntpd services are active on the system will synchronize its time to a dedicated time server. This is important whether the system is configured to be a client (and synchronize only its own clock) or it is also acting as a time server for other systems. Synchronizing time is essential for authentication services such as Kerberos, but it is also important for maintaining accurate logs and auditing possible security breaches.

bash fix

```
if which systemctl &> /dev/null
then
  if systemctl list-unit-files | grep -q timesyncd &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep timesyncd | sed "s/^\(\s\+\)\?//" | cut -d" " -f1 )
  elif systemctl list-unit-files | grep -qE "chrony(d)?\." &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "chrony(d)?\." | sed "s/^\(\s\+\)\?//" | cut -d"
" -f1 )
  elif systemctl list-unit-files | grep -qE "\bntp\b" &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "\bntp\b" | sed "s/^\(\s\+\)\?//" | cut -d" "
-f1 )
  else
    # install chrony
    if [[ "$OS_LIKE" == "fedora" ]]
    then
      yum -y install chrony &> /dev/null
      SERVICE=$( systemctl list-units | grep chrony | sed "s/^\(\s\+\)\?//" | cut -d" " -f1 )
    elif [[ "$OS_LIKE" == "debian" ]]
    then
      apt-get -y install chrony &> /dev/null
```

```
      SERVICE=$( systemctl list-units | grep chrony | sed "s/^\(\s\+\)\?//" | cut -d" " -f1 )
    elif [[ "$OS_LIKE" == "suse" ]]
    then
      zypper --non-interactive install ntp &> /dev/null
      SERVICE=$( systemctl list-unit-files | grep "\bntp\b" | sed "s/^\(\s\+\)\?//" | cut -d" " -f1
)
    else
      echo "could not install chrony on system"
      exit 1
    fi
  fi
  if ! systemctl is-enabled $SERVICE &> /dev/null
  then
    systemctl enable $SERVICE &> /dev/null
  fi
  if ! systemctl is-active $SERVICE &> /dev/null
  then
    systemctl start $SERVICE &> /dev/null
  fi
else
  echo "system does not use systemctl, manual installation of time sync will be required"
  exit 1
fi
```

NASA-ASCS-20178: Set Password Hashing Algorithm in /etc/libuser.conf

NASA ASCS ID	NASA-ASCS-20178
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	SC-13, IA-07
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.5.4
MITRE ATT&CK Reference	TA0006, T1003, M1041

Some systems use the `libuser` package, if the system is using it, it should be configured properly. In the `libuser.conf` manpage:

```
login_defs
  A  path  to the login.defs file from shadow.  If this variable is defined, the variables from the
named file are used in place of some libuser variables.  Variables explicitly defined in
libuser.conf are not affected by contents of login.defs.
  ...
  ENCRYPT_METHOD       | defaults/crypt_style
```

The `libuser.conf` file if it exists, it should ensure it points to `login.defs` and not specify the `crypt_style`.

Since the login.defs file will not be affected by the libuser.conf, it is allowed to have `crypt_style = sha512` for the purspose of compliance, or to have the value commented out.

In `/etc/libuser.conf`, add or correct the following line:

In the `[import]` section:

```
login_defs = /etc/login.defs
```

In its `[defaults]` section

```
# crypt_style = sha512
```

Rationale

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 that are encrypted with a weak algorithm are no more protected than if they are kept in plain text. This setting ensures user and group account administration utilities are configured to store only encrypted representations of passwords. Additionally, the crypt_style configuration option ensures the use of a strong hashing algorithm that makes password cracking attacks more difficult.

bash fix

```
if [ -e /etc/libuser.conf ]
then
  LIBUSER_CONF="/etc/libuser.conf"
  LOGIN_DEFS_REGEX='[[:space:]]*\[import](.*(\n)+)+?[[:space:]]*login_defs[[:space:]]*'

  # Try find login_defs in the [source] section, if not existing,
  # If it isn't here, then add it to [defaults] section.
  if grep -qzosP $LOGIN_DEFS_REGEX $LIBUSER_CONF ; then
    sed -i "s/\(login_defs[[:space:]]*=[[:space:]]*\).*/\1\/etc\/login.defs/g" $LIBUSER_CONF
  elif grep -qs "\[import]" $LIBUSER_CONF ; then
    sed -i "/[[:space:]]*\[import]/a login_defs = \/etc\/login.defs" $LIBUSER_CONF
  else
    echo -e "[import]\nlogin_defs = \/etc\/login.defs" >> $LIBUSER_CONF
  fi

  CRYPT_STYLE_REGEX='[[:space:]]*\[defaults](.*(\n)+)+?[[:space:]]*crypt_style[[:space:]]*'
  # Try find crypt_style in [defaults] section. Comment it out if it exists
  if grep -qzosP $CRYPT_STYLE_REGEX $LIBUSER_CONF ; then
    sed -i "s/\(crypt_style[[:space:]]*=[[:space:]]*.*\).*/#\1/g" $LIBUSER_CONF
  fi
fi
```

NASA-ASCS-20179: Set Password Hashing Algorithm in /etc/login.defs

NASA ASCS ID	NASA-ASCS-20179
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	SC-13, IA-07
STIG Reference	RHEL_8_STIG RHEL-08-010110
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.5.4
MITRE ATT&CK Reference	TA0006, T1003, M1041

In `/etc/login.defs` , add or correct the following line to ensure the system will use SHA-512 as the hashing algorithm:

```
ENCRYPT_METHOD SHA512
```

Rationale

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

bash fix

```
if grep -E --silent "^\bENCRYPT_METHOD\b" /etc/login.defs
then
    sed -i "s/^\bENCRYPT_METHOD\b.*/ENCRYPT_METHOD SHA512/" /etc/login.defs
else
    echo "" >> /etc/login.defs
    echo "ENCRYPT_METHOD SHA512" >> /etc/login.defs
fi
```

NASA-ASCS-20180: Set PAMs Password Hashing Algorithm

NASA ASCS ID	NASA-ASCS-20180
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	SC-13, IA-07
STIG Reference	RHEL_8_STIG RHEL-08-010130, RHEL_8_STIG RHEL-08-010160, RHEL_8_STIG RHEL-08-010159

CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.5.4
MITRE ATT&CK Reference	TA0006, T1003, M1041

The PAM system service can be configured to only store encrypted representations of passwords. In `/etc/pam.d/system-auth`, the `password` section of the file controls which PAM modules execute during a password change. Set the `pam_unix.so` module in the `password` section to include the argument `sha512` , as shown below:

```
password    sufficient    pam_unix.so sha512 other arguments...
```

When local users change their passwords, hashes for the new passwords shall be generated using the SHA-512 algorithm.

In modern distributions the use of `yescrypt` is also permitted. The `yescrypt` algorithm provide PBKDF2 and SHA256 mechanisms that are NIST approved.

If `pam_unix.so` is disabled by the OS to enforce multi-factor authentication, the compliance check will regard the missing value as a pass.

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-update`. Refer to distribution documentation for appropriate configuration use. The PIV-SSSD Handbook has both `authselect` and `pam-auth-update` content that can also help.

Rationale

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 that are encrypted with a weak algorithm are no more protected than if they are kept in plain text. This setting ensures user and group account administration utilities are configured to store only encrypted representations of passwords. Additionally, the crypt_style configuration option ensures the use of a strong hashing algorithm that makes password cracking attacks more difficult.

bash fix

```
# NOTE: Use of authselect tool requires System Administrator to fix. See note in specification
document.
```

NASA-ASCS-20190: Disable Kernel Parameter for Accepting ICMP Redirects for All Interfaces

NASA ASCS ID	NASA-ASCS-20190
Severity	**High**
Group	network/system

NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040280, RHEL_8_STIG RHEL-08-040279, RHEL_8_STIG RHEL-08-040209
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.2
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv4.conf.all.accept_redirects` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.all.accept_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.all.accept_redirects = 0
```

Rationale

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. This feature of the IPv4 protocol has few legitimate uses.

bash fix

```
# Set runtime for net.ipv4.conf.all.accept_redirects
/sbin/sysctl -q -n -w net.ipv4.conf.all.accept_redirects=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.all.accept_redirects"
SED_INLINE="s/^net.ipv4.conf.all.accept_redirects.*$/net.ipv4.conf.all.accept_redirects=0/"
ECHO_APPEND="net.ipv4.conf.all.accept_redirects=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20191: Disable Kernel Parameter for Accepting Source-Routed Packets for All Interfaces

NASA ASCS ID	NASA-ASCS-20191

Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040240, RHEL_8_STIG RHEL-08-040239
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.1
MITRE ATT&CK Reference	TA0007, T1018, T1590, T1590.005
Control Setting	0

To set the runtime status of the `net.ipv4.conf.all.accept_source_route` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.all.accept_source_route=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.all.accept_source_route = 0
```

Rationale

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. Accepting source-routed packets in the IPv4 protocol has few legitimate uses.

bash fix

```
# Set runtime for net.ipv4.conf.all.accept_source_route
/sbin/sysctl -q -n -w net.ipv4.conf.all.accept_source_route=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.all.accept_source_route"
SED_INLINE="s/^net.ipv4.conf.all.accept_source_route.*$/net.ipv4.conf.all.accept_source_route=0/"
ECHO_APPEND="net.ipv4.conf.all.accept_source_route=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20192: Disable Kernel Parameter for Sending ICMP Redirects for All Interfaces

NASA ASCS ID	NASA-ASCS-20192
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040220
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.2.2
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv4.conf.all.send_redirects` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.all.send_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.all.send_redirects = 0
```

Rationale

Internet Control Message Protocol (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. The ability to send ICMP redirects is only appropriate for systems acting as routers.

bash fix

```
# Set runtime for net.ipv4.conf.all.send_redirects
/sbin/sysctl -q -n -w net.ipv4.conf.all.send_redirects=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.all.send_redirects"
SED_INLINE="s/^net.ipv4.conf.all.send_redirects.*$/net.ipv4.conf.all.send_redirects=0/"
ECHO_APPEND="net.ipv4.conf.all.send_redirects=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20193: Disable Kernel Parameter for Accepting ICMP Redirects By Default

NASA ASCS ID	NASA-ASCS-20193
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040210, RHEL_8_STIG RHEL-08-040209, RHEL_8_STIG RHEL-08-040279
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.2
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv4.conf.default.accept_redirects` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.default.accept_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.default.accept_redirects = 0
```

Rationale

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. This feature of the IPv4 protocol has few legitimate uses.

bash fix

```
# Set runtime for net.ipv4.conf.default.accept_redirects
/sbin/sysctl -q -n -w net.ipv4.conf.default.accept_redirects=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.default.accept_redirects"
SED_INLINE="s/^net.ipv4.conf.default.accept_redirects.*$/net.ipv4.conf.default.accept_redirects=0/"
ECHO_APPEND="net.ipv4.conf.default.accept_redirects=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
```

```
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20194: Disable Kernel Parameter for Accepting Source-Routed Packets By Default

NASA ASCS ID	NASA-ASCS-20194
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040250, RHEL_8_STIG RHEL-08-040249
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.1
MITRE ATT&CK Reference	TA0007, T1018, T1590, T1590.005
Control Setting	0

To set the runtime status of the `net.ipv4.conf.default.accept_source_route` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.default.accept_source_route=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.default.accept_source_route = 0
```

Rationale

Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. Accepting source-routed packets in the IPv4 protocol has few legitimate uses. It should be disabled unless it is absolutely required, such as when IPv4 forwarding is enabled and the system is legitimately functioning as a router.

bash fix

```
# Set runtime for net.ipv4.conf.default.accept_source_route
/sbin/sysctl -q -n -w net.ipv4.conf.default.accept_source_route=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.default.accept_source_route"
SED_INLINE="s/^net.ipv4.conf.default.accept_source_route.*$/net.ipv4.conf.default.accept_source_rou
te=0/"
ECHO_APPEND="net.ipv4.conf.default.accept_source_route=0"
```

```
if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20195: Disable Kernel Parameter for Sending ICMP Redirects by Default

NASA ASCS ID	NASA-ASCS-20195
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040270
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.2.2
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv4.conf.default.send_redirects` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.default.send_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.default.send_redirects = 0
```

Rationale

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. The ability to send ICMP redirects is only appropriate for systems acting as routers.

bash fix

```
# Set runtime for net.ipv4.conf.default.send_redirects
/sbin/sysctl -q -n -w net.ipv4.conf.default.send_redirects=0

CONFIG_FILE=/etc/sysctl.conf
```

```
EXISTS_IF_REGEX="^net.ipv4.conf.default.send_redirects"
SED_INLINE="s/^net.ipv4.conf.default.send_redirects.*$/net.ipv4.conf.default.send_redirects=0/"
ECHO_APPEND="net.ipv4.conf.default.send_redirects=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20196: Enable Kernel Parameter to Ignore ICMP Broadcast Echo Requests

NASA ASCS ID	NASA-ASCS-20196
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040230
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.5
MITRE ATT&CK Reference	TA0007, T1018, T1590, T1590.005
Control Setting	1

To set the runtime status of the `net.ipv4.icmp_echo_ignore_broadcasts` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Rationale

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks. Ignoring ICMP echo requests (pings) sent to broadcast or multicast addresses makes the system slightly more difficult to enumerate on the network.

bash fix

```
# Set runtime for net.ipv4.icmp_echo_ignore_broadcasts
```

```
/sbin/sysctl -q -n -w net.ipv4.icmp_echo_ignore_broadcasts=1

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.icmp_echo_ignore_broadcasts"
SED_INLINE="s/^net.ipv4.icmp_echo_ignore_broadcasts.*$/net.ipv4.icmp_echo_ignore_broadcasts=1/"
ECHO_APPEND="net.ipv4.icmp_echo_ignore_broadcasts=1"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20197: Verify that Shared Library Files Have Restrictive Permissions

NASA ASCS ID	NASA-ASCS-20197
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
STIG Reference	RHEL_8_STIG RHEL-08-010330
MITRE ATT&CK Reference	T1083, M1022
MITRE D3FEND Reference	D3-LFP

System-wide shared library files, which are linked to executables during process load time or run time, are stored in the following directories by default:

```
/lib
/lib64
/usr/lib
/usr/lib64
```

Kernel modules, which can be added to the kernel during runtime, are stored in `/lib/modules` . All files in these directories should not be group-writable or world-writable. If any file in these directories is found to be group-writable or world-writable, correct its permission with the following command:

```
$ chmod go-w FILE
```

Rationale

Files from shared library directories are loaded into the address space of processes (including privileged ones) or of

the kernel itself at runtime. Restrictive permissions are necessary to protect the integrity of the system.

bash fix

```
DIRS="/lib /lib64 /usr/lib /usr/lib64"

for dirPath in $DIRS
do
  find "$dirPath" -perm /022 -type f -not -name libfreeblpriv3.chk -not -name libsoftokn3.chk -not
-name libnssdbm3.chk -exec chmod go-w '{}' \;
done
```

NASA-ASCS-20207: Ensure firewall is Active for IPv4

NASA ASCS ID	NASA-ASCS-20207
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-07 (12), AC-17 (1)
STIG Reference	RHEL_8_STIG RHEL-08-040100, RHEL_8_STIG RHEL-08-040101
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.4.1.4
MITRE ATT&CK Reference	M1037

Ensure the system is running firewall for IPv4.

Applications such as `firewalld` and `ufw` which leverages `iptables` or `ebtables` in a more intuitive management structure and are recommended for firewall management.

Red Hat Enterprise Linux and it’s clones run the Firewall Daemon application.

For `firewalld`:

```
#> systemctl enable firewalld.service
```

Ubuntu Linux uses the Uncomplicated Firewall application.

```
#> systemctl enable ufw.service
```

SUSE Linux Enterprise uses the SuSEfireall2 application.

```
#> systemctl enable SuSEfirewall2.service
```

Otherwise base firewall services can be managed directly.

`iptables.service` is also available when not running a full firewall management software.

```
#> systemctl enable iptables.service
```

`ebtables.service` is also available when not running a full firewall management software.

```
#> systemctl enable ebtables.service
```

Rationale

Systems connected to a network are susceptible to threats that can be prevented with proper blocking of network ports using a firewall.

bash fix

```
if which systemctl &> /dev/null
then
  if which firewalld &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?firewalld\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  elif which ufw &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?ufw\.service" | sed "s/^\s\+//" | cut
-d" " -f1 )
  elif which SuSEfirewall2 &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?SuSEfirewall2\.service" | sed
"s/^\s\+//" | cut -d" " -f1 )
  elif which ebtables &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?ebtables\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  else
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?iptables\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  fi
  systemctl enable $SERVICE &> /dev/null
  systemctl start $SERVICE &> /dev/null
else
  if which firewalld &> /dev/null
  then
    SERVICE=$( chkconfig | grep "^firewalld" | cut -d" " -f1 )
  else
    SERVICE=$( chkconfig | grep "^iptables" | cut -d" " -f1 )
  fi
  chkconfig $SERVICE on &> /dev/null
  service $SERVICE start &> /dev/null
fi
```

NASA-ASCS-20219: Verify Group Who Owns shadow File

NASA ASCS ID	NASA-ASCS-20219
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AU-09
MITRE ATT&CK Reference	T1547, M1022
MITRE D3FEND Reference	D3-LFP, D3-SCP

To properly set the group owner of `/etc/shadow` , run the command:

For Red Hat based systems

```
chgrp root /etc/shadow
```

For Ubuntu based systems

```
chgrp shadow /etc/shadow
```

Rationale

The `/etc/shadow` file stores password hashes. Protection of this file is critical for system security.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  chgrp root /etc/shadow &> /dev/null
elif [[ "$OS_LIKE" == "debian" ]]
then
  chgrp shadow /etc/shadow &> /dev/null
elif [[ "$OS_LIKE" == "suse" ]]
then
  chgrp shadow /etc/shadow &> /dev/null
fi
```

NASA-ASCS-20245: Remove NIS Client

NASA ASCS ID	NASA-ASCS-20245
Severity	**High**

Group	obsolete/services
MITRE ATT&CK Reference	M1042

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (`ypbind`) was used to bind a system to an NIS server and receive the distributed configuration files.

Rationale

The NIS service is an inherently insecure system that has been vulnerable to DOS attacks and buffer overflows; it also has poor authentication for querying NIS maps. NIS is generally replaced by other protocols, such as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q ypbind &> /dev/null
  then
    yum -y remove ypbind &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' yp-tools )" == "installed" ]]
  then
    apt-get -y purge yp-tools &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q ypbind &> /dev/null
  then
    zypper --non-interactive remove ypbind &> /dev/null
  fi
fi
```

NASA-ASCS-20263: Ensure Software Patches Installed

NASA ASCS ID	NASA-ASCS-20263
Severity	**High**
Group	software/system
NIST SP 800-53r5 Reference	SI-02 (c)
STIG Reference	RHEL_8_STIG RHEL-08-010010
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.9

MITRE ATT&CK Reference	TA0002, TA0004, M1028
MITRE D3FEND Reference	D3-SU

If the system is joined to a vendor supported software repository, or organizational supported repository clone, and all software patching remains current to vendor supplied versions.

This control is measured outside of the standard specification.

On `yum` based systems:

```
yum update
```

On `apt` based systems:

```
apt-get update
apt-get dist-upgrade
```

On `zypp` based systems:

```
zypper update
```

Non-compliance is monitored and measured outside of this specification, no CDM check will be shown for this control in reports.

Rationale

Installing software updates is a fundamental mitigation against the exploitation of publicly-known vulnerabilities. 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.

bash fix

```
if which yum &> /dev/null
then
  yum update -y &> /dev/null
elif which apt &> /dev/null
then
  apt-get update &> /dev/null
  #apt-get -y dist-upgrade &> /dev/null
  DEBIAN_FRONTEND='noninteractive' apt-get -y -o Dpkg::Options::='--force-confdef' -o
Dpkg::Options::='--force-confold' dist-upgrade &> /dev/null
elif which zypper &> /dev/null
then
  zypper --non-interactive update &> /dev/null
fi
```

NASA-ASCS-20268: Disable Accepting IPv6 Redirects By Default

NASA ASCS ID	NASA-ASCS-20268
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040280, RHEL_8_STIG RHEL-08-040210
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.2
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv6.conf.all.accept_redirects` kernel parameter, run the following command:

```
sysctl -w net.ipv6.conf.all.accept_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv6.conf.all.accept_redirects = 0
```

Rationale

An illicit ICMP redirect message could result in a man-in-the-middle attack.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "0" ]]
then
  /sbin/sysctl -q -n -w net.ipv6.conf.all.accept_redirects=0
  CONFIG_FILE=/etc/sysctl.conf
  EXISTS_IF_REGEX="^net.ipv6.conf.all.accept_redirects"
  SED_INLINE="s/^net.ipv6.conf.all.accept_redirects.*$/net.ipv6.conf.all.accept_redirects=0/"
  ECHO_APPEND="net.ipv6.conf.all.accept_redirects=0"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-20269: Disable Accepting IPv6 Router Advertisements

NASA ASCS ID	NASA-ASCS-20269
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040262, RHEL_8_STIG RHEL-08-040261
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.9
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv6.conf.default.accept_ra` kernel parameter, run the following command:

```
sysctl -w net.ipv6.conf.default.accept_ra=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv6.conf.default.accept_ra = 0
```

Rationale

An illicit router advertisement message could result in a man-in-the-middle attack.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "0" ]]
then
  /sbin/sysctl -q -n -w net.ipv6.conf.default.accept_ra=0

  CONFIG_FILE=/etc/sysctl.conf
  EXISTS_IF_REGEX="^net.ipv6.conf.default.accept_ra"
  SED_INLINE="s/^net.ipv6.conf.default.accept_ra.*$/net.ipv6.conf.default.accept_ra=0/"
  ECHO_APPEND="net.ipv6.conf.default.accept_ra=0"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
```

```
fi
```

NASA-ASCS-20270: Disable Accepting IPv6 Redirects By Default

NASA ASCS ID	NASA-ASCS-20270
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040210, RHEL_8_STIG RHEL-08-040280
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.2
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv6.conf.default.accept_redirects` kernel parameter, run the following command:

```
sysctl -w net.ipv6.conf.default.accept_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv6.conf.default.accept_redirects = 0
```

Rationale

An illicit ICMP redirect message could result in a man-in-the-middle attack.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "0" ]]
then
  /sbin/sysctl -q -n -w net.ipv6.conf.default.accept_redirects=0

  CONFIG_FILE=/etc/sysctl.conf
  EXISTS_IF_REGEX="^net.ipv6.conf.default.accept_redirects"

SED_INLINE="s/^net.ipv6.conf.default.accept_redirects.*$/net.ipv6.conf.default.accept_redirects=0/"
  ECHO_APPEND="net.ipv6.conf.default.accept_redirects=0"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
```

```
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-20271: Disable Kernel Parameter for Accepting IPv6 Source-Routed Packets for Interfaces By Default

NASA ASCS ID	NASA-ASCS-20271
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040250
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.1
MITRE ATT&CK Reference	TA0007, T1018, T1590, T1590.005
Control Setting	0

To set the runtime status of the `net.ipv6.conf.default.accept_source_route` kernel parameter, run the following command:

```
sysctl -w net.ipv6.conf.default.accept_source_route=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv6.conf.default.accept_source_route = 0
```

Rationale

Source-routed packets allow the source of the packet to suggest 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 traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router. Accepting source-routed packets in the IPv6 protocol has few legitimate uses.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "0" ]]
then
  /sbin/sysctl -q -n -w net.ipv6.conf.default.accept_source_route=0
```

```
  CONFIG_FILE=/etc/sysctl.conf
  EXISTS_IF_REGEX="^net.ipv6.conf.default.accept_source_route"

SED_INLINE="s/^net.ipv6.conf.default.accept_source_route.*$/net.ipv6.conf.default.accept_source_rou
te=0/"
  ECHO_APPEND="net.ipv6.conf.default.accept_source_route=0"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-20273: Disable Kernel Parameter for Accepting IPv6 Source-Routed Packets for All Interfaces

NASA ASCS ID	NASA-ASCS-20273
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-05
STIG Reference	RHEL_8_STIG RHEL-08-040240
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.1
MITRE ATT&CK Reference	TA0007, T1018, T1590, T1590.005
Control Setting	0

To set the runtime status of the `net.ipv6.conf.all.accept_source_route` kernel parameter, run the following command:

```
sysctl -w net.ipv6.conf.all.accept_source_route=0
```

If this is not the system default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv6.conf.all.accept_source_route = 0
```

Rationale

Source-routed packets allow the source of the packet to suggest 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 traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.

Accepting source-routed packets in the IPv6 protocol has few legitimate uses.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "0" ]]
then
  CONFIG_FILE=/etc/sysctl.conf
  EXISTS_IF_REGEX="^net.ipv6.conf.all.accept_source_route"
  SED_INLINE="s/^net.ipv6.conf.all.accept_source_route.*$/net.ipv6.conf.all.accept_source_route=0/"
  ECHO_APPEND="net.ipv6.conf.all.accept_source_route=0"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-20274: Ensure firewall is Enabled for IPv6

NASA ASCS ID	NASA-ASCS-20274
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-07 (12), AC-17 (1)
STIG Reference	RHEL_8_STIG RHEL-08-040100
MITRE ATT&CK Reference	M1037

Ensure the system is running firewall for IPv6.

Applications such as `firewalld` and `ufw` which leverages `ip6tables` or `ebtables` in a more intuitive management structure and are recommended for firewall management.

Red Hat Enterprise Linux and it's clones run the Firewall Daemon application.

For `firewalld`:

```
#> systemctl enable firewalld.service
```

Ubuntu Linux uses the Uncomplicated Firewall application.

```
#> systemctl enable ufw.service
```

SUSE Linux Enterprise uses the SuSEfireall2 application.

```
#> systemctl enable SuSEfirewall2.service
```

Otherwise base firewall services can be managed directly.

`ip6tables.service` is also available when not running a full firewall management software.

```
#> systemctl enable ip6tables.service
```

`ebtables.service` is also available when not running a full firewall management software.

```
#> systemctl enable ebtables.service
```

Rationale

Systems connected to a network are susceptible to threats that can be prevented with proper blocking of network ports using a firewall.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "1" ]]
then
  echo "IPv6 disabled, skipping"
elif which systemctl &> /dev/null
then
  if which firewalld &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?firewalld\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  elif which ufw &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?ufw\.service" | sed "s/^\s\+//" | cut
-d" " -f1 )
  elif which SuSEfirewall2 &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?SuSEfirewall2\.service" | sed
"s/^\s\+//" | cut -d" " -f1 )
  elif which ebtables &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?ebtables\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  else
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?ip6tables\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  fi
  systemctl enable $SERVICE &> /dev/null
  systemctl start $SERVICE &> /dev/null
```

```
else
  if which firewalld &> /dev/null
  then
    SERVICE=$( chkconfig | grep "^firewalld" | cut -d" " -f1 )
  else
    SERVICE=$( chkconfig | grep "^ip6tables" | cut -d" " -f1 )
  fi
  chkconfig $SERVICE on &> /dev/null
  service $SERVICE start &> /dev/null
fi
```

NASA-ASCS-20279: Ensure Mandatory Access Controls Are Not Disabled in /etc/default/grub

NASA ASCS ID	NASA-ASCS-20279
Severity	**High**
Group	mandatory_access_control
NIST SP 800-53r5 Reference	AC-03 (3)
MITRE D3FEND Reference	D3-SCP

The Mandatory Access Control can be disabled at boot time by an argument in `/etc/default/grub`. Remove any instances of the disable flag from the kernel arguments in that file to prevent it from being disabled at boot.

In SELinux systems remove any `selinux=0` or `enforce=0` values from `/etc/default/grub`.

In AppArmor systems remove and `apparmor=0` value from `/etc/default/grub`.

Additional information on kernel parameters can be found here: https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html

Additional information on grub configuration can be found here: https://www.gnu.org/software/grub/manual/grub/html_node/Simple-configuration.html#Simple-configuration

Rationale

Disabling a major host protection feature, such as Mandatory Access Controls, at boot time prevents it from confining system services at boot time. Further, it increases the chances that it will remain off during system operation.

bash fix

```
if ! which aa-status &> /dev/null
then
  sed -i --follow-symlinks "s/selinux=0//gI" /etc/default/grub /etc/grub2.cfg /etc/grub.d/*
  sed -i --follow-symlinks "s/enforcing=0//gI" /etc/default/grub /etc/grub2.cfg /etc/grub.d/*
```

```
else
  sed -i --follow-symlinks "s/apparmor=0//gI" /etc/default/grub /etc/grub2.cfg /etc/grub.d/*
fi

MKCONFIG=$( which {grub,grub2}-mkconfig 2> /dev/null )
for GRUBCFG in $( find /boot -name grub.cfg )
do
  $MKCONFIG -o $GRUBCFG
done
```

NASA-ASCS-20280: Ensure Mandatory Access Control Policy is Loaded

NASA ASCS ID	NASA-ASCS-20280
Severity	**High**
Group	mandatory_access_control
NIST SP 800-53r5 Reference	AC-03 (3)
STIG Reference	RHEL_8_STIG RHEL-08-010450
MITRE D3FEND Reference	D3-SCP
Control Setting	targeted

The Mandatory Access Control system provides additional security to Linux systems by constraining a subject from access to an object. In conjunction with Discretionary Access Control, they provides a Multilevel Security profile. The SELinux or AppArmor services shall be enabled on Linux systems to provide the Mandatory Access Control.

In SELinux the `/etc/selinux/config` value for `SELINUXTYPE` to `targeted` or `mls`.

Policies, such as `mls` , provide additional security labeling and greater confinement but are not compatible with many general-purpose use cases.

In AppArmor ensure that the systemd service is enabled and active.

Rationale

Setting the Mandatory Access Control policy ensures the system will confine processes that are likely to be targeted for exploitation, such as network or system services.

bash fix

```
if which sestatus &> /dev/null
then
  CONFIG_FILE=/etc/sysconfig/selinux
  EXISTS_IF_REGEX="^SELINUXTYPE"
  SED_INLINE="s/^SELINUXTYPE.*$/SELINUXTYPE=targeted/"
  ECHO_APPEND="SELINUXTYPE=targeted"
```

```
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
elif which aa-status &> /dev/null
then
  systemctl enable apparmor &> /dev/null
  systemctl start apparmor &> /dev/null
fi
```

NASA-ASCS-20281: Ensure Mandatory Access Control is Enforcing

NASA ASCS ID	NASA-ASCS-20281
Severity	**High**
Group	mandatory_access_control
NIST SP 800-53r5 Reference	AC-03 (3)
STIG Reference	RHEL_8_STIG RHEL-08-010170
MITRE D3FEND Reference	D3-SCP
Control Setting	enforcing

Ensure that the Mandatory Access Control policies are set to enforcing.

In SELinux ensure that `/etc/selinux/config` has `SELINUX` value set to enforcing.

In AppArmor ensure that all profiles are being enforced.

The remediation uses a command to enforce all profiles `aa-enforce /etc/apparmor.d/*` that may not always work as expected. In cases that it does not enforce all the policies, it may be a matter of enforcing some individually. Known profiles that have been shown to not work with the global enforcement and have to be individually enforced are `usr.lib.libreoffice.program.oosplash` and `usr.lib.libreoffice.program.soffice.bin`.

In Ubuntu the `apparmor-utils` package is needed for access to `aa-enforce`

Rationale

Setting the Mandatory Access Control state to enforcing ensures the confinement of potentially compromised processes to the security policy, which is designed to prevent them from causing damage to the system or further elevating their privileges.

bash fix

```
if which sestatus &> /dev/null
then
  CONFIG_FILE=/etc/selinux/config
  EXISTS_IF_REGEX="^(\s+)?SELINUX(\s+)?="
  SED_INLINE="s/^SELINUX=.*$/SELINUX=enforcing/"
  ECHO_APPEND="SELINUX=enforcing"

  if [[ $( grep -iE $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
elif which aa-status &> /dev/null
then
  aa-enforce /etc/apparmor.d/*
fi
```

NASA-ASCS-20282: Ensure gpg Signature is Enforcing in Package Management

NASA ASCS ID	NASA-ASCS-20282
Severity	**High**
Group	software/system
NIST SP 800-53r5 Reference	SI-07 (15)
STIG Reference	RHEL_8_STIG RHEL-08-010370
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.2.3
MITRE ATT&CK Reference	M1045, T1554

Repository signatures need always be checked prior to installation of a package on a system. Set or remove values from the package management configuration to prevent the system from allowing untrusted sources being used to install software.

In `yum` based configurations, set the `gpgcheck` value to `1` in the `/etc/yum.conf` file.

In `apt` based configurations, ensure that the string `AllowInsecureRepository` and `AllowDowngradeInsecureRepository` are missing or set to `false`.

In `zypper` based configurations, ensure that the `repo_gpgcheck` is not set to off, use the default by ensuring any lines with `gpgcheck` such as `repo_gpgcheck` are commented out.

This check deprecates NASA-ASCS-20042

Rationale

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software provider has not been tampered with and that it has been provided by a trusted vendor. Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor.

bash fix

```
if which yum &> /dev/null
then
  CONFIG_FILE=/etc/yum.conf
  EXISTS_IF_REGEX="^gpgcheck"
  SED_INLINE="s/^gpgcheck.*$/gpgcheck=1/"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  fi
elif which apt &> /dev/null
then
  if grep -E "Allow(DowngradeTo)?InsecureRepository.*true" /etc/apt/apt.conf.d/*
  then
    apt -o Acquire::AllowInsecureRepositories=false -o
Acquire::AllowDowngradeToInsecureRepositories=false update
  fi
elif which zypper &> /dev/null
then
  CONFIG_FILE=/etc/zypp/zypp.conf
  EXISTS_IF_REGEX="^(\s+)?repo_gpgcheck"
  SED_INLINE="s/^(\s+)?(repo_gpgcheck.*)$/# \2/I"

  if [[ $( grep -iE $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  fi
fi
```

NASA-ASCS-20360: Install the auditd Service

NASA ASCS ID	NASA-ASCS-20360
Severity	**High**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-12
STIG Reference	RHEL_8_STIG RHEL-08-030180

MITRE ATT&CK Reference	M1047

The `auditd` service shall be installed.

Installing the `audit` service:

```
yum install audit
```

On debian based systems:

```
apt-get install auditd
```

Rationale

The auditd service is an access monitoring and accounting daemon, watching system calls to audit any access.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if ! rpm -q audit &> /dev/null
  then
    yum install audit -y
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' auditd )" != "installed" ]]
  then
    apt-get install auditd -y
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if ! rpm -q auditd &> /dev/null
  then
    zypper install auditd -y
  fi
fi
```

NASA-ASCS-20368: Ensure Default SNMP Password Is Not Used

NASA ASCS ID	NASA-ASCS-20368
Severity	**High**
Group	snmp/services
MITRE ATT&CK Reference	T1078.001

Edit `/etc/snmp/snmpd.conf` by removing or changing the default community strings of `public` and `private`. Once the default community strings have been changed, issue the following command to restart the SNMP service:

```
$ sudo service snmpd restart
```

Rationale

Whether or not they are active, default simple network management protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default SNMP community strings, this allows anyone to gather data about the system and the network. This information can be used to aid and attacker in potentially compromising the information system and network components.

bash fix

```
if grep -s "public\|private" /etc/snmp/snmpd.conf | grep -qv "^#"; then
    sed -i "/^\s*#/b;/public\|private/ s/^/#/" /etc/snmp/snmpd.conf
fi
```

NASA-ASCS-20369: Ensure firewall management application is installed

NASA ASCS ID	NASA-ASCS-20369
Severity	**High**
Group	network/system
NIST SP 800-53r5 Reference	SC-07 (12), AC-17 (1)
STIG Reference	RHEL_8_STIG RHEL-08-040100
MITRE ATT&CK Reference	M1037

Applications like `firewalld` and `ufw` are typically loaded in the default system installation. If finding that the application is not loaded, the following commands can be executed to load them.

On Red Hat based systems

```
yum install firewalld
```

On Ubuntu based systems

```
apt-get install ufw
ufw allow ssh
ufw enable
```

On SUSE systems

```
zypper install SuSEfirewall2
```

On Amazon 2 systems, selinux will need updated for `firewalld` to function properly

SELinux profile

```
#============= firewalld_t ==============

#!!!! This avc is allowed in the current policy
allow firewalld_t proc_t:filesystem getattr;

#!!!! This avc is allowed in the current policy
allow firewalld_t self:capability net_raw;

#!!!! This avc is allowed in the current policy
allow firewalld_t self:rawip_socket { create getopt setopt };

#!!!! This avc is allowed in the current policy
allow firewalld_t usermodehelper_t:file { open read };
```

SELinux boolean

```
setsebool -P domain_kernel_load_modules 1
```

Rationale

Modern Linux distributions offer firewall management packages that provide strong firewall configuration. Use of incorrectly configured firewalls can open a system up to undesired attacks from the network. Firewall configurations can be difficult, and the management applications provide a safer method to properly configure the firewall.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  yum install firewalld -y &> /dev/null
elif [[ "$OS_LIKE" == "debian" ]]
then
  apt-get install ufw -y &> /dev/null
elif [[ "$OS_LIKE" == "suse" ]]
then
  zypper --non-interactive install SuSEfirewall2 &> /dev/null
fi
```

NASA-ASCS-20372: Remove NOPASSWD:ALL values in sudo configurations

NASA ASCS ID	NASA-ASCS-20372
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	IA-02
STIG Reference	RHEL_8_STIG RHEL-08-010380
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 5.3.4
MITRE ATT&CK Reference	T1574, T1078
MITRE D3FEND Reference	D3-SPP, D3-AM

When the operating system provide the capability to change user authenticators, change security roles, or escalate a functional capability, it is critical the user reauthenticate.

The `sudoer` configurations provide the option to allow unauthenticated privilage escalation with the keywords of `NOPASSWD` and `!authenticate`. Ensure these values are not configured to use the `ALL` alias in the `/etc/sudoers` or `/etc/sudoers.d/*` files.

Rationale

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

NASA-ASCS-20376: Enable Task Schedule Service

NASA ASCS ID	NASA-ASCS-20376
Severity	**High**
Group	cron_and_at/services

Task scheduling services are used to execute commands at preconfigured times. It is required by almost all systems to perform necessary maintenance tasks, such as notifying root of system activity. Services such as `cron`, `anacron`, and `systemd-timers` are available in modern Linux systems to provide methods to schedule task events to run.

Checking for active services using `systemd` can use the following commands:

systemd-timers

```
systemctl list-timers
```

cron

```
systemctl list-units cron.service
```

The `anacron` service should be used with mobile devices since it will execute scheduled actions when systems return from a powered off state (as opposed to `cron` which will only trigger on the scheduled time allotment).

anacron

```
systemctl list-units anacron.timer
```

Rationale

Due to its usage for maintenance and security-supporting tasks, enabling a task scheduler is essential.

bash fix

```
# Since systemd should have timers by default, only add cron if timers is no available
if ! systemctl status timers.target > /dev/null
then
  if which systemctl &> /dev/null
  then
    SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?cron(d)?\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
    systemctl enable $SERVICE &> /dev/null
    systemctl start $SERVICE &> /dev/null
  else
    SERVICE=$( chkconfig | grep "^cron" | cut -d" " -f1 )
    chkconfig $SERVICE on &> /dev/null
    service $SERVICE start &> /dev/null
  fi
fi
```

NASA-ASCS-20377: Limit Password Reuse

NASA ASCS ID	NASA-ASCS-20377
Severity	**High**
Group	accounts/system
NIST SP 800-53r5 Reference	IA-05
STIG Reference	RHEL_8_STIG RHEL-08-020220, RHEL_8_STIG RHEL-08-020221
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.5.3
MITRE ATT&CK Reference	TA0006, M1027, T1078
MITRE D3FEND Reference	D3-SPP
Control Setting	24

Passwords will not be reused for recent history. The `remember` keyword in the `pam_pwhistory.so` PAM module manages this.

This replaces the NASA-ASCS-20128 control that allowed for `pam_unix.so` to also be used. However, the pam_unix.so used `md5` hashing which is not sufficient for current distributions. The man page for `pam_unix.so` currently states to use the `pam_pwhistory.so` module instead.

`pam_pwhistory.so` will likely need to be added to the system.

In the files `/etc/pam.d/`, append `remember=24` to the line which refers to the `pam_pwhistory.so` module, as shown below:

```
password required pam_pwhistory.so ...existing_options... remember=24
password required pam_unix.so ... use_authtok
```

Due to potential lock out issue with PAM, no automated remediation is provided in this control.

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-update`. Refer to distribution documentation for appropriate configuration use. The PIV-SSSD Handbook has both `authselect` and `pam-auth-update` content that can also help.

Rationale

Preventing reuse of previous passwords helps ensure that a compromised password is not reused by a user.

bash fix

```
# NOTE: Use of authselect tool requires System Administrator to fix. See note in specification
document.
```

NASA-ASCS-40035: (OpenSSH) Configure SSH Banner with NASA IT System Use Notification

NASA ASCS ID	NASA-ASCS-40035
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	AC-08
STIG Reference	RHEL_8_STIG RHEL-08-010040
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.15
Control Setting	/etc/issue

This setting ensures that remote users see and must agree to the NASA IT System Use Notification before authentication is allowed.

The default configuration for OpenSSH does not display a warning banner or notification.

To configure the setting for OpenSSH, insert the OS-specific value into the following line and then add or correct this line in the sshd_config file on the system:

```
Banner /etc/issue
```

OS-specific values are defined in the ASCS Specification for each OS.

Rationale

Using the NASA IT System Use Notification text for the SSH warning banner reinforces policy awareness during the login process and facilitates possible legal action against attackers.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^Banner"
SED_INLINE="s/^Banner.*$/Banner /etc/issue/"
ECHO_APPEND="Banner /etc/issue"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40042: (OpenSSH) Disable Host-Based Authentication

NASA ASCS ID	NASA-ASCS-40042

Severity	**High**
Group	ssh/services
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.8
MITRE ATT&CK Reference	M1042, T1078
Control Setting	no

This setting specifies whether `rhosts` or `/etc/hosts.equiv` authentication together with successful public key client host authentication is allowed (host-based authentication).

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
HostbasedAuthentication no
```

Rationale

SSH trust relationships mean a compromise on one host can allow an attacker to move to other trusted hosts without needing authentication. Additionally, host-based authentication does not permit configuring command restrictions or limits on what can be done on the destination server when accessed. Because of this, it is not recommended for automated access. It is not recommended for interactive users either, because it does not present an interactive login. This would not be considered a good practice, especially for accounts with elevated privileges.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^HostbasedAuthentication"
SED_INLINE="s/^HostbasedAuthentication.*$/HostbasedAuthentication no/"
ECHO_APPEND="HostbasedAuthentication no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
```

```
fi
```

NASA-ASCS-40045: (OpenSSH) Use Only Strong Host Key Algorithms

NASA ASCS ID	NASA-ASCS-40045
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-08 (1)
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENCR
Control Setting	ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256

This setting specifies the host key signature algorithms that the server offers.

To configure the setting for OpenSSH, insert the OS-specific value into the following line and then add or correct this line in the sshd_config file on the system:

```
HostKeyAlgorithms ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256
```

OS-specific values are defined in the ASCS Specification for each OS.

Rationale

Weak host key algorithms have been shown to be susceptible to counterfeit or collision attacks that can lead to system compromise.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^HostKeyAlgorithms"
SED_INLINE="s/^HostKeyAlgorithms.*$/HostKeyAlgorithms ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256/"
ECHO_APPEND="HostKeyAlgorithms ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256"
```

```
INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40048: (OpenSSH) Disable SSH Support for .rhosts Files

NASA ASCS ID	NASA-ASCS-40048
Severity	**High**
Group	ssh/services
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.11
MITRE ATT&CK Reference	T1078, M1042
Control Setting	yes

This setting specifies whether to ignore per-user `.rhosts` and `.shosts` files during HostbasedAuthentication.

The system-wide `/etc/hosts.equiv` and `/etc/shosts.equiv` are still used regardless of this setting.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
IgnoreRhosts yes
```

Rationale

SSH trust relationships mean a compromise on one host can allow an attacker to move to other trusted hosts without needing authentication.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^IgnoreRhosts"
SED_INLINE="s/^IgnoreRhosts.*$/IgnoreRhosts yes/"
ECHO_APPEND="IgnoreRhosts yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40051: (OpenSSH) Disable Kerberos Authentication

NASA ASCS ID	NASA-ASCS-40051
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	IA-02
STIG Reference	RHEL_8_STIG RHEL-08-010521
MITRE ATT&CK Reference	M1042, M1032
MITRE D3FEND Reference	D3-MFA
Control Setting	no

This setting specifies whether the password provided by the user for PasswordAuthentication will be validated through the Kerberos Key Distribution Center (KDC).

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
KerberosAuthentication no
```

Rationale

With PasswordAuthentication disabled to enforce Multi-Factor Authentication, this setting would not be relevant.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^KerberosAuthentication"
SED_INLINE="s/^KerberosAuthentication.*$/KerberosAuthentication no/"
ECHO_APPEND="KerberosAuthentication no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40054: (OpenSSH) Set Time to Disconnect During Login

NASA ASCS ID	NASA-ASCS-40054
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-05 (2)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.19
MITRE ATT&CK Reference	T1499
Control Setting	120

This setting ensures that the server disconnects if the user has not successfully logged in within the defined amount of time.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
LoginGraceTime  120
```

OS-specific values are defined in the ASCS Specification for each OS.

Rationale

Unbound login sessions can be a vector of attack (e.g., a Denial of Service (DoS) attack). As such, user interactive login methods need to have a bounded time set before disconnecting.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^LoginGraceTime"
SED_INLINE="s/^LoginGraceTime.*$/LoginGraceTime 120/"
ECHO_APPEND="LoginGraceTime 120"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40055: (OpenSSH) Set LogLevel to VERBOSE

NASA ASCS ID	NASA-ASCS-40055
Severity	**High**
Group	ssh/services

NIST SP 800-53r5 Reference	AC-17 (1), AU-02
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.5
MITRE D3FEND Reference	D3-OSM
Control Setting	VERBOSE

This setting configures the verbosity level that is used when logging messages from `sshd`. The Agency required setting is VERBOSE. By default, this configuraiton is set to INFO.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
LogLevel VERBOSE
```

Rationale

SSH provides several logging optios with varying levels of verbosity. Setting the logging level to VERBOSE is required because it produces logs with all necessary, security-relevant information while not violating the privacy of users.

The INFO level provides too little detail to be useful in incident response efforts. Conversely, the DEBUG level provides so much data that it is difficult to identify important, security-relevant information, and this level of logging violates the privacy of users.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^LogLevel"
SED_INLINE="s/^LogLevel.*$/LogLevel VERBOSE/"
ECHO_APPEND="LogLevel VERBOSE"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
```

```
fi
```

NASA-ASCS-40060: (OpenSSH) Disable Password Authentication

NASA ASCS ID	NASA-ASCS-40060
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	IA-02 (1)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.6
MITRE ATT&CK Reference	M1032
MITRE D3FEND Reference	D3-MFA
Control Setting	no

This setting specifies whether password authentication is allowed.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PasswordAuthentication     no
```

Rationale

Use of smartcard authentication is mandatory at the Agency.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PasswordAuthentication"
SED_INLINE="s/^PasswordAuthentication.*$/PasswordAuthentication no/"
ECHO_APPEND="PasswordAuthentication no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
```

```
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40062: (OpenSSH) Disable SSH Root Login

NASA ASCS ID	NASA-ASCS-40062
Severity	**High**
Group	ssh/services
STIG Reference	RHEL_8_STIG RHEL-08-010550
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.7
MITRE ATT&CK Reference	T1078.001
MITRE D3FEND Reference	D3-AM
Control Setting	no

This setting specifies whether root can log in using `ssh`.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PermitRootLogin no
```

Rationale

Setting this configuration to `no` ensures that root is not able to log in. Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy to prevent access directly as root. In addition, accessing the system with a user-specific account provides individual accountability for actions performed and helps to minimize direct attack attempts on the root account password.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PermitRootLogin"
SED_INLINE="s/^PermitRootLogin.*$/PermitRootLogin no/"
ECHO_APPEND="PermitRootLogin no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
```

```
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40063: (OpenSSH) Disable Override of User Environment Options

NASA ASCS ID	NASA-ASCS-40063
Severity	**High**
Group	ssh/services
STIG Reference	RHEL_8_STIG RHEL-08-010830
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.10
MITRE ATT&CK Reference	T1098, M1042
Control Setting	no

This setting specifies whether `~/.ssh/environment` and `environment=` options in `~/.ssh/authorized_keys` are processed by `sshd`.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PermitUserEnvironment no
```

Rationale

Enabling environment processing may enable users to bypass access restrictions in some configurations using mechanisms such as LD_PRELOAD.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PermitUserEnvironment"
```

```
SED_INLINE="s/^PermitUserEnvironment.*$/PermitUserEnvironment no/"
ECHO_APPEND="PermitUserEnvironment no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40065: (OpenSSH) Set the Standard Network Port

NASA ASCS ID	NASA-ASCS-40065
Severity	**High**
Group	ssh/services
Control Setting	22

This setting specifies the port number that `sshd` listens on.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
Port    22
```

Rationale

By requiring port `22` use for SSH, the Agency can better monitor traffic and identify potential malicious behavior on the network.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^Port"
SED_INLINE="s/^Port.*$/Port 22/"
```

```
ECHO_APPEND="Port 22"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40070: (OpenSSH) Enable Public Key Authentication

NASA ASCS ID	NASA-ASCS-40070
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	IA-02 (1), IA-02 (2)
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENCR
Control Setting	yes

This setting specifies whether public key authentication is allowed.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PubkeyAuthentication   yes
```

`PubkeyAuthentication` is required for PIV authentication.

Rationale

Public key authentication is a strong authentication method.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PubkeyAuthentication"
SED_INLINE="s/^PubkeyAuthentication.*$/PubkeyAuthentication yes/"
ECHO_APPEND="PubkeyAuthentication yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40075: (OpenSSH) Enable Use of Strict Modes Checking

NASA ASCS ID	NASA-ASCS-40075
Severity	**High**
Group	ssh/services
STIG Reference	RHEL_8_STIG RHEL-08-010500
MITRE ATT&CK Reference	T1036
Control Setting	yes

This setting specifies whether `sshd` checks file modes and ownership of the user's files and home directory before accepting login.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
StrictModes yes
```

Rationale

If users have access to modify user-specific SSH configuration files, they may be able to log into the system as another user.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^StrictModes"
SED_INLINE="s/^StrictModes.*$/StrictModes yes/"
ECHO_APPEND="StrictModes yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40076: (OpenSSH) Set Logging on Subsystem for Secure File Transfer

NASA ASCS ID	NASA-ASCS-40076
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	AU-02
MITRE D3FEND Reference	D3-OSM
Control Setting	sftp /usr/libexec/openssh/sftp-server -f AUTHPRIV -l INFO

Configures the subsystem for file transfer with appropriate flags for logging.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
Subsystem    sftp /usr/libexec/openssh/sftp-server -f AUTHPRIV -l INFO
```

OS-specific values are defined in the ASCS Specification for each OS.

This control is dependent on the rsyslog facility. The use of the AUTH or AUTHPRIV corresponds with the rsyslog configuration to identify the resultant log file inclusion.

It is the responsibility of the ISO to ensure that all necessary log entries are being monitored. For ensuring that the log entries go to the /var/log/secure location, make sure that the sshd_config SyslogFacility entry for AUTH or AUTHPRIV corresponds with the rsyslog.conf entry auth.* or authpriv.*.

As an example, the default RHEL7 implementation of rsyslog will have *.info and authpriv.none for /var/log/messages stated in the /etc/rsyslog.conf configuration. This ensures that no entry for AUTHPRIV will be in the /var/log/messages file, but any INFO-related entry will be. As with the sshd_config SyslogFacility, if the value is set to AUTH, then this will result in any auth.info messages ending up in /var/log/messages.

Rationale

Logging to AUTHPRIV facility makes it easier for administrators to see relevant errors and successes. Use of the AUTHPRIV facility will also assist log aggregation tools.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^Subsystem"

if [[ "$OS_LIKE" == "fedora" ]]
then
  SFTP_LIBS=$(rpm -q $(rpm -q --whatprovides $(which sshd)) --dump | grep sftp-server | grep -Ev
"(man|doc|\.build-id)" | awk '{print $1}' | sed "s/\//\\\\\//g" )
elif [[ "$OS_LIKE" == "debian" ]]
then
  SFTP_LIBS=$( dpkg-query -S sftp-server | grep -Ev "(man|doc|\.build-id)" | grep sftp-server | awk
'{print $2}' | sed "s/\//\\\\\//g" )
elif [[ "$OS_LIKE" == "suse" ]]
then
  SFTP_LIBS=$(rpm -q $(rpm -q --whatprovides $(which sshd)) --dump | grep sftp-server | grep -Ev
"(man|doc|\.build-id)" | awk '{print $1}' | sed "s/\//\\\\\//g" )
fi

for SFTP_LIB in ${SFTP_LIBS[*]}
do
  if [ ! -h $SFTP_LIB ]
  then
    SED_INLINE="s/^Subsystem.*$/Subsystem sftp $SFTP_LIB -f AUTH -l INFO/"
    ECHO_APPEND="Subsystem sftp $SFTP_LIB -f AUTH -l INFO"

    INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
    if ls $INCLUDES &> /dev/null
```

```
    then
      CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
    fi
    FIXED=1
    for CONFIG_FILE in ${CONFFILES[*]}
    do
      if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
      then
        sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
        FIXED=0
      fi
    done
    if [[ "$FIXED" != "0" ]]
    then
      [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
      echo $ECHO_APPEND >> $CONFIG_FILE
    fi
  fi
done
```

NASA-ASCS-40078: (OpenSSH) Set Syslog Facility

NASA ASCS ID	NASA-ASCS-40078
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	AU-02
MITRE D3FEND Reference	D3-OSM
Control Setting	AUTH or AUTHPRIV

The `sshd` service uses the host logging facility, the `SyslogFacility` dictates the destination logging to use. The `AUTH` or `AUTHPRIV` facility will result in logging to the host authentication logs (i.e. `/var/log/secure`).

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
SyslogFacility   AUTH or AUTHPRIV
```

This control is dependent on the rsyslog facility, the use of the `AUTH` or `AUTHPRIV` corresponds with the rsyslog configuration to identify the resultant log file inclusion.

It is the responsibility of the System Owner to ensure that the proper entries into the logs are able to be monitored. For ensuring that the log entries go to the `/var/log/secure` location, make sure that the sshd_config SyslogFacility entry for `AUTH` or `AUTHPRIV` corresponds with the rsyslog.conf

> entry `auth.*` or `authpriv.\*`.
>
> As an example, the default RHEL7 implementation of rsyslog will have `*.info` and `authpriv.none` for /var/log/messages stated in the /etc/rsyslog.conf configuration. This ensures that no entry for `AUTHPRIV` will be in the `/var/log/messages` file, but any `INFO`-related entry will be. As with the sshd_config `SyslogFacility`, if the value is set to `AUTH`, then this will result in any auth.info messages ending up in `/var/log/messages`.

Rationale

Logging to the `AUTHPRIV` facility makes it easier for administrators to see relevant errors and successes. Use of the `AUTHPRIV` facility will also assist log aggregation tools.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^SyslogFacility"
SED_INLINE="s/^SyslogFacility.*$/SyslogFacility AUTHPRIV/"
ECHO_APPEND="SyslogFacility AUTHPRIV"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40079: (OpenSSH) Enable TCP KeepAlive

NASA ASCS ID	NASA-ASCS-40079
Severity	**High**
Group	ssh/services
Control Setting	yes

This setting specifies whether the system sends TCP keepalive messages to the client.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
TCPKeepAlive     yes
```

Rationale

Maintaining keepalive messages provides the server with assurance of persistent connection to the connected client. The server will notice if the network goes down or the client host crashes, thereby preventing infinitely hanging sessions.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^TCPKeepAlive"
SED_INLINE="s/^TCPKeepAlive.*$/TCPKeepAlive yes/"
ECHO_APPEND="TCPKeepAlive yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40081: (OpenSSH) Disable Login Usage

NASA ASCS ID	NASA-ASCS-40081
Severity	**High**
Group	ssh/services
Control Setting	no

This setting specifies if sshd is to pass environment control to the login mechanism to process post-login functions during interactive login sessions.

UseLogin has been deprecated since version 7.4p1. Adding the setting will cause sshd to generate unwanted log messages.

To configure the setting for OpenSSH in versions prior to 7.4p1, add or correct the following line in the sshd_config file on the system:

```
UseLogin     no
```

Rationale

Post-login features are best handled by sshd and not handed over to other operating system services.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^UseLogin"
SED_INLINE="s/^UseLogin.*$/UseLogin no/"
ECHO_APPEND="UseLogin no"

if [[ "$( sshd -T -C user=root -C host=localhost -C addr=localhost | grep uselogin )" != "" ]]
then
  INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
  if ls $INCLUDES &> /dev/null
  then
    CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
  fi
  FIXED=1
  for CONFIG_FILE in ${CONFFILES[*]}
  do
    if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
    then
      sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
      FIXED=0
    fi
  done
  if [[ "$FIXED" != "0" ]]
  then
    [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-40087: (OpenSSH) Verify Permissions on SSH Server Private Key Files

NASA ASCS ID	NASA-ASCS-40087
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.1
MITRE ATT&CK Reference	T1083, M1022
MITRE D3FEND Reference	D3-LFP

To properly set the permissions of the SSH Server Private Key Files, run the command:

```
```

OS-specific values are defined in the ASCS Specification for each OS.

Rationale

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

bash fix

```
if [ $(uname) == "Darwin" ]
then
  for KEYFILE in /etc/ssh/*_key
  do
    chmod 600 "$KEYFILE"
  done
else
  for KEYFILE in /etc/ssh/*_key
  do
    if [[ "$( stat -c "%G" $KEYFILE )" == "ssh_keys" ]]
    then
      chmod 640 $KEYFILE
    else
      chmod 600 $KEYFILE
    fi
  done
fi
```

NASA-ASCS-40089: (OpenSSH) Verify Permissions on SSH Server Public Key Files

NASA ASCS ID	NASA-ASCS-40089
Severity	**High**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (4)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.3
MITRE ATT&CK Reference	T1083, M1022
MITRE D3FEND Reference	D3-LFP

To properly set the permissions of the SSH Server Public Key Files, run the command:

```
```

OS-specific values are defined in the ASCS Specification for each OS.

Rationale

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

bash fix

```
for KEYFILE in /etc/ssh/*.pub
do
  chmod 644 $KEYFILE &> /dev/null
done
```

NASA-ASCS-40093: (OpenSSH) Configure SSH to opt out of System Crypto Policy

NASA ASCS ID	NASA-ASCS-40093
Severity	**High**
Group	software/system
NIST SP 800-53r5 Reference	SC-08 (1), IA-07, AC-17 (2)
STIG Reference	RHEL_8_STIG RHEL-08-010287
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.14
MITRE ATT&CK Reference	M1041

MITRE D3FEND Reference	D3-MENCR

Crypto policies provide centralized control over crypto algorithms used by many packages. SSH is supported by crypto policy, but the SSH configuration may be set up to opt-out of the policy enforcement. To ensure that the ASCS controls that are managed in the crypto policies are not ignored, ASCS suggests to opt-out for ssh, but will accept FIPS crypto policy if choosing to do so.

It is not clear if by setting FIPS as the `CRYPTO_POLICY` all ASCS controls will be configured as expected, which is the reason for the options to opt-out for SSH policy and rely on the direct ssh settings.

To check that crypto policies is being opted out, ensure that the `CRYPTO_POLICY` variable is not set to any value in the `/etc/sysconfig/sshd`.

`/etc/sysconfig/sshd`

```
CRYPTO_POLICY=
```

Rationale

Using the system crypto policy makes the behavior of the SSH service ignore the `MACs` and `Ciphers` settings in the `sshd_config` controls used by ASCS,

bash fix

```
if which update-crypto-policies &> /dev/null
then
  if grep -E "^(\s+)?CRYPTO_POLICY" /etc/sysconfig/sshd 2> /dev/null
  then
    sed -i -E "s/^(\s+)?CRYPTO_POLICY.*$/CRYPTO_POLICY=/" /etc/sysconfig/sshd
  else
    echo "CRYPTO_POLICY=" >> /etc/sysconfig/sshd
  fi
fi
```

NASA-ASCS-40559: (Linux Desktop) Disable User List on Display Manager

NASA ASCS ID	NASA-ASCS-40559
Severity	**High**
Group	software/displaymanager
STIG Reference	RHEL_8_STIG RHEL-08-020032
MITRE ATT&CK Reference	T1589

In the default graphical environment, users logging in directly to the system are greeted with a login screen that

displays all known users. Disable the user list on the display manager.

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40562: (Linux Desktop) Disable GUI Guest Login

NASA ASCS ID	NASA-ASCS-40562
Severity	**High**
Group	software/system
MITRE ATT&CK Reference	T1078.001

Configure the Display Managers to require access with valid credentials by ensuring that the "guest" accounts feature is disabled.

See [_configuration_options] for remediation guides for desktop environments and display managers.

Rationale

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

NASA-ASCS-40565: (Linux Desktop) Ensure Display Manager Banner is Enabled

NASA ASCS ID	NASA-ASCS-40565
Severity	**High**
Group	software/displaymanager
NIST SP 800-53r5 Reference	AC-08

Configure the display manager to provide a warning banner text that is required for any U.S. Government information system.

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40566: (Linux Desktop) Ensure Display Manager Provides the Proper Message Banner

NASA ASCS ID	NASA-ASCS-40566
Severity	**High**
Group	software/displaymanager

NIST SP 800-53r5 Reference	AC-08
STIG Reference	RHEL_8_STIG RHEL-08-010050

Configure the display manager to provide the official login warning banner required by all U.S. Government information systems.

Set the banner text with current NASA accepted NASA IT System Use Notification

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40567: (Linux Desktop) Set the Login Number of Failures to the GUI Display Manager

NASA ASCS ID	NASA-ASCS-40567
Severity	**High**
Group	software/system
NIST SP 800-53r5 Reference	AC-07
MITRE ATT&CK Reference	T1110, M1027

Configure the display manager to restart the authentication process after 3 failed attempts.

See [_configuration_options] for remediation guides for desktop environments and display managers.

Rationale

Setting the password retry prompts that are permitted on a per-session basis to a low value requires some software, such as SSH, to re-connect. This can slow down and draw additional attention to some types of password guessing attacks.

NASA-ASCS-40568: (Linux Desktop) Enable Screen Lock

NASA ASCS ID	NASA-ASCS-40568
Severity	**High**
Group	software/desktop
NIST SP 800-53r5 Reference	AC-11
STIG Reference	RHEL_8_STIG RHEL-08-020030

Configure the desktop environment to enable the screen lock feature or screensaver to require authentication upon returning to active use.

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40569: (Linux Desktop) Enable Screen Lock Idle Delay

NASA ASCS ID	NASA-ASCS-40569
Severity	**High**
Group	software/desktop
NIST SP 800-53r5 Reference	AC-11
STIG Reference	RHEL_8_STIG RHEL-08-020060

Configure the desktop environment to enable the screen lock feature or screensaver to initiate when the desktop session has been idle. The maximum allowable idle time is 15 minutes.

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40715: (OpenSSH) Disable AllowAgentForwarding

NASA ASCS ID	NASA-ASCS-40715
Severity	**High**
Group	ssh/services
MITRE ATT&CK Reference	T1563
Control Setting	no

This setting specifies whether a host will allow the continued forwarding of an SSH agent socket. By default configuration, the `sshd` service will allow the SSH Agent to forward a socket to subsiquent hosts. The `AllowAgentForwarding` control is expected to be set to `no` in order to prevent lateral movement in the network without reauthenticating.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
AllowAgentForwarding no
```

Alternatively it is acceptable to disable forwarding:

```
DisableForwarding yes
```

The advantages of Agent forwarding for administrators can be provided by the ProxyJump feature using AllowTcpForwarding. While the client side will require some additional flags or configuration files to attain the same simplicity, the use of client SSH Agent is not the major

> threat. With the use of the forwarding connection through a host using the ProxyJump option, each host is directly authenticated at the client and this prevents the potential of having a socket hijacked at an intermediate host.

Rationale

Allowing a server to forward the SSH agent on to another host presents a vector for lateral movement without requiring actual authentication. In the configuration of enforcing the PIV credential, this is more so as the PIV identity is also forwarded. If an intermediate host is compromised, the socket for forwarded credential can be hijacked and used to impersonate a PIV holder during a login session to access other hosts in the network using the same credential.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^AllowAgentForwarding"
SED_INLINE="s/^AllowAgentForwarding.*$/AllowAgentForwarding no/"
ECHO_APPEND="AllowAgentForwarding no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40716: (OpenSSH) Disable Keyboard Interactive Authentication

NASA ASCS ID	NASA-ASCS-40716
Severity	**High**
Group	ssh/services
NIST SP 800-53r5 Reference	IA-02

MITRE ATT&CK Reference	T1556, M1042
MITRE D3FEND Reference	D3-MFA
Control Setting	no

This setting specifies whether keyboard interactive authentication is allowed. By default configuration, the `sshd` service will allow PAM password authentication via keyboard entry. Set the `KbdInteractiveAuthentication` setting to `no`.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
KbdInteractiveAuthentication no
```

MFA solutions typically also use `KbdInteractiveAuthentication`. Agency-approved MFA solutions are permitted to set this control to other than `no` without being scored as non-compliant.

As of OpenSSH v9.x, this setting replaces the deprecated `ChallengeResponseAuthentication` setting.

Rationale

Setting this control to `no` ensures that passwords are not permissible for authentication.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^KbdInteractiveAuthentication"
SED_INLINE="s/^KbdInteractiveAuthentication.*$/KbdInteractiveAuthentication no/"
ECHO_APPEND="KbdInteractiveAuthentication no"

if [[ "$( sshd -T -C user=root -C host=localhost -C addr=localhost | grep
kbdinteractiveauthentication )" != "" ]]
then
  INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
  if ls $INCLUDES &> /dev/null
  then
    CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
  fi
  FIXED=1
  for CONFIG_FILE in ${CONFFILES[*]}
  do
    if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
    then
      sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
      FIXED=0
    fi
  done
  if [[ "$FIXED" != "0" ]]
```

```
  then
    [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

5.3. Medium Severity Settings

Medium severity settings ***SHALL*** be adhered to, as they are monitored, scored, and reported to NASA.

- *Medium* severity settings target any vulnerability which, if exploited, has the potential to result in the loss of confidentiality, integrity, or availability.

NASA-ASCS-20379: Ensure Local System is Enforcing for Multi-Factor Authentication

NASA ASCS ID	NASA-ASCS-20379
Severity	**Medium**
Group	accounts/system
NIST SP 800-53r5 Reference	IA-02
STIG Reference	RHEL_8_STIG RHEL-08-020250, RHEL_8_STIG RHEL-08-010400
MITRE ATT&CK Reference	M1032
MITRE D3FEND Reference	D3-MFA

Ensuring that local authentication is enforcing Multi-Factor Authentication (MFA).

This control is similar to NASA-ASCS-20375 Ensure System is Enforcing PIV Authentication.

PIV Authentication is considered MFA, passing NASA-ASCS-20375 will also pass this control.

Along with PIV options, this control will also consider systems with RSA SecurID or RADIUS MFA.

The internal website https://cset.nasa.gov/ has links to multiple options regarding PIV solutions at the Agency.

Rationale

The 2021 Executive Order on Cybersecurity has identified Multi-Factor Authentication as a requirement for all Federal IT Systems.

NASA-ASCS-40681: (OpenSSH) Configure Remote Access Multi-Factor Authentication

NASA ASCS ID	NASA-ASCS-40681
Severity	**Medium**
Group	ssh/auth
NIST SP 800-53r5 Reference	IA-02
MITRE ATT&CK Reference	M1032
MITRE D3FEND Reference	D3-MFA

Configure OpenSSH to enforce Multi-Factor Authentication (MFA) for remote access.

Currently, NASA officially supports MFA using the Personal Identity Verification (PIV)-SSH and RSA SecurID.

See CSET's Handbooks for supporting guidance.

Rationale

Federal systems are required to enforce MFA. Use of single-factor authentication has proven to be insufficient to protect against modern threats.

5.4. Low Severity Settings

Low severity settings are expected to be implemented unless there is a justifiable cause not to. Deviations from security configuration settings with a Low severity rating will not impact a system's compliance score.

- *Low* severity settings target any vulnerability which, if exploited, degrades measures to protect against the loss of confidentiality, integrity, or availability.
- *Low* severity settings often pertain to the principle of least privilege, (vendor- or ASCS-determined) best practices, or other measures aimed at protecting exploitable avenues.

Carefully assess the environment prior to implementing any setting with a Low severity rating. Low severity settings may conflict with settings that have a higher severity rating, cause instability in some specialized environments, and/or contain configurations that cannot be accurately scanned and reported by NASA.

NASA-ASCS-20001: Set Account Expiration Following Inactivity

NASA ASCS ID	NASA-ASCS-20001
Severity	**Low**
Group	accounts/system

NIST SP 800-53r5 Reference	AC-02 (3)
STIG Reference	RHEL_8_STIG RHEL-08-020260
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.6.1.4
MITRE ATT&CK Reference	TA0001, T1078, M1027
MITRE D3FEND Reference	D3-AL, D3-LAM
Control Setting	35

To specify the number of days after a password expires (which signifies inactivity) until an account is permanently disabled, add or correct the following lines in `/etc/default/useradd`, substituting `NUM_DAYS` appropriately:

```
INACTIVE= 35
```

A value of `35` is recommended. If a password is currently on the verge of expiration, then 35 days remain until the account is automatically disabled. However, if the password will not expire for another 60 days, then 95 days could elapse until the account would be automatically disabled. See the `man useradd` from console for more information. Determining the inactivity timeout must be done with careful consideration regarding what would be considered "normal" periods of inactivity in the respective environment.

Rationale

Disabling inactive accounts ensures they are not available to attackers.

bash fix

```
CONFIG_FILE=/etc/default/useradd
EXISTS_IF_REGEX="^INACTIVE="
SED_INLINE="s/^INACTIVE=.*$/INACTIVE=35/"
ECHO_APPEND="INACTIVE=35"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20004: Ensure the Default Bash Umask is Set Correctly

NASA ASCS ID	NASA-ASCS-20004
Severity	**Low**
Group	accounts/system

STIG Reference	RHEL_8_STIG RHEL-08-020353
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.6.5
Control Setting	077

To ensure the default umask for users of the Bash Shell is set properly, add or correct the `umask` setting in `/etc/bashrc` to read as follows:

```
umask  077
```

Rationale

The `umask` value influences the permissions assigned to files when they are created. A misconfigured `umask` value could result in files with excessive permissions allowing unauthorized users read or write access.

bash fix

```
CONFIG_FILE=/etc/bashrc
EXISTS_IF_REGEX="^umask"
SED_INLINE="s/^umask.*$/umask 077/"
ECHO_APPEND="umask 077"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20005: Ensure the Default Umask is Set Correctly in login.defs

NASA ASCS ID	NASA-ASCS-20005
Severity	**Low**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-020351
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.6.5
Control Setting	077

To ensure the default umask controlled by `/etc/login.defs` is set properly, add or correct the `UMASK` setting in `/etc/login.defs` to read as follows:

```
UMASK  077
```

Rationale

The umask value influences the permissions assigned to files when they are created. A misconfigured umask value could result in files with excessive permissions that can be read and written to by unauthorized users.

bash fix

```
CONFIG_FILE=/etc/login.defs
EXISTS_IF_REGEX="^\bUMASK\b"
SED_INLINE="s/^UMASK\s.*$/UMASK 077/"
ECHO_APPEND="UMASK 077"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20006: Ensure the Default Umask is Set Correctly in /etc/profile

NASA ASCS ID	NASA-ASCS-20006
Severity	**Low**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-020353
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.6.5
Control Setting	077

To ensure the default umask controlled by `/etc/profile` is set properly, add or correct the `umask` setting in `/etc/profile` to read as follows:

```
umask  077
```

Rationale

The umask value influences the permissions assigned to files when they are created. A misconfigured umask value could result in files with excessive permissions that can be read or written to by unauthorized users.

bash fix

```
CONFIG_FILE=/etc/profile
EXISTS_IF_REGEX="^\bumask\b"
SED_INLINE="s/^umask.*$/umask 077/"
ECHO_APPEND="umask 077"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
```

```
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20007: Configure auditd Max Log File Size

NASA ASCS ID	NASA-ASCS-20007
Severity	**Low**
Group	auditing/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.2.1
Control Setting	320

Edit the file `/etc/audit/auditd.conf`. Add or modify the following line:

```
max_log_file = 320
```

Set the value to `320` (MB) or higher for general-purpose systems. Larger values support retention of even more audit data.

The value for `320` is determined from the current baseline of what values are audited. We observed that with the current baseline, `8` MB will monitor approximately 2 hours of regular workstation use. Based on `320` MB, the monitored time will extend to 80 hours, or approx 3.3 days. With `ROTATE` set on `5` log files, the coverage of audit logs will be over 15 days.

Rationale

The total storage for audit log files must be large enough to retain log information over the period required. This is a function of the maximum log file size and the number of logs retained.

bash fix

```
AUDITCONFIG=/etc/audit/auditd.conf
AUDITCONF_ITEM="max_log_file"
AUDITCONF_VALUE="320"

if [[ "$(grep -E "^(\s+)?$AUDITCONF_ITEM(\s+)?=(\s+)?.*$" $AUDITCONFIG)" ]]
then
  sed -i
"s/^\(\s\+\)\?$AUDITCONF_ITEM\(\s\+\)\?=\(\s\+\)\?.*$/\1$AUDITCONF_ITEM\2=\3$AUDITCONF_VALUE/"
$AUDITCONFIG
else
  echo "$AUDITCONF_ITEM = $AUDITCONF_VALUE" >> $AUDITCONFIG
fi
```

NASA-ASCS-20008: Configure auditd Number of Logs Retained

NASA ASCS ID	NASA-ASCS-20008
Severity	**Low**
Group	auditing/system
Control Setting	5

Edit the file `/etc/audit/auditd.conf`. Add or modify the following line to the correct value of `5`:

```
num_logs = 5
```

Rationale

The total storage for audit log files must be large enough to retain log information over the period required. This is a function of the maximum log file size and the number of logs retained.

bash fix

```
var_auditd_num_logs="5"

AUDITCONFIG=/etc/audit/auditd.conf

grep -q ^num_logs $AUDITCONFIG && \
  sed -i 's/^num_logs.*/num_logs = '"$var_auditd_num_logs"'/g' $AUDITCONFIG
if ! [ $? -eq 0 ]; then
  echo "num_logs = $var_auditd_num_logs" >> $AUDITCONFIG
fi
```

NASA-ASCS-20018: Disable Odd Job Daemon (oddjobd)

NASA ASCS ID	NASA-ASCS-20018
Severity	**Low**
Group	base/services

The `oddjobd` service exists to provide an interface and access control mechanism through which specified privileged tasks can run tasks for unprivileged client applications. The `oddjobd` service shall be disabled with the following command:

```
$ systemctl disable oddjobd.service
```

Rationale

The oddjobd service may provide necessary functionality in some environments, and shall be disabled if it's not needed. Execution of tasks by privileged programs, on behalf of unprivileged ones, has traditionally been a source of

privilege escalation security issues.

bash fix

```
SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?oddjob(d)?\.service" | cut -d" " -f1 )
if [[ "$SERVICE" != "" ]]
then
  systemctl disable $SERVICE &> /dev/null
  systemctl stop $SERVICE &> /dev/null
fi
```

NASA-ASCS-20019: Disable Network Router Discovery Daemon (rdisc)

NASA ASCS ID	NASA-ASCS-20019
Severity	**Low**
Group	base/services
MITRE ATT&CK Reference	T1499

The `rdisc` service implements the client side of the ICMP Internet Router Discovery Protocol (IRDP), which allows discovery of routers on the local subnet. If a router is discovered, then the local routing table is updated with a corresponding default route.

The threat of having the `rdisc` system active is that an attacker can inject (adversary-in-the-middle) routes that do not exist, this can create a situation that the system can become unavailable (Denial of Service Attack).

The `rdisc` service is be disabled with the following command:

```
$ systemctl disable rdisc.service
```

or

```
chkconfig rdisc off
```

Rationale

General-purpose systems typically have their network and routing information configured statically by a system administrator. Workstations and some special-purpose systems often use Dynamic Host Configuration Protocol (DHCP) (instead of IRDP) to retrieve dynamic network configuration information.

bash fix

```
if which systemctl &> /dev/null
then
  SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?rdisc(d)?\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  if systemctl is-active $SERVICE &> /dev/null
```

```
  then
    systemctl stop $SERVICE &> /dev/null
  fi
  if systemctl is-enabled $SERVICE &> /dev/null
  then
    systemctl disable $SERVICE &> /dev/null
  fi
else
  SERVICE=$( chkconfig | grep "^rdisc" | cut -d" " -f1 )
  chkconfig $SERVICE off &> /dev/null
  service $SERVICE stop &> /dev/null
fi
```

NASA-ASCS-20022: Ensure the root User PATH Variable Does Not Include World or Group-Writable Directories

NASA ASCS ID	NASA-ASCS-20022
Severity	**Low**
Group	accounts/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.7
MITRE ATT&CK Reference	T1574.007, M1038
MITRE D3FEND Reference	D3-LFP

For each element in root's path, run:

```
# ls -ld DIR
```

Ensure that write permissions are disabled for group and other.

Rationale

Such entries increase the risk that root could execute code provided by unprivileged users and malicious actors.

NASA-ASCS-20023: Ensure the Default C Shell Umask is Set Correctly

NASA ASCS ID	NASA-ASCS-20023
Severity	**Low**
Group	accounts/system
STIG Reference	RHEL_8_STIG RHEL-08-020353

Control Setting	077

To ensure the default umask for users of the C shell is set properly, add or correct the `umask` setting in `/etc/csh.cshrc` to read as follows:

```
umask  077
```

Rationale

The umask value influences the permissions assigned to files when they are created. A misconfigured umask value could result in files with excessive permissions that can be read or written to by unauthorized users.

bash fix

```
CONFIG_FILE=/etc/csh.cshrc
EXISTS_IF_REGEX="^\bumask\b"
SED_INLINE="s/^umask.*$/umask 077/"
ECHO_APPEND="umask 077"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
var_accounts_user_umask="077"

grep -q umask /etc/csh.cshrc && \
  sed -i "s/umask.*/umask $var_accounts_user_umask/g" /etc/csh.cshrc
if ! [ $? -eq 0 ]; then
    echo "umask $var_accounts_user_umask" >> /etc/csh.cshrc
fi
```

NASA-ASCS-20035: Configure auditd max_log_file_action Upon Reaching Maximum Log Size

NASA ASCS ID	NASA-ASCS-20035
Severity	**Low**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-05
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.2.2
Control Setting	rotate

The default action to take when the logs reach their maximum size of at least 6 MB is to rotate the log files,

discarding the oldest one. To configure the action taken by `auditd`, add or correct the line in `/etc/audit/auditd.conf`:

```
max_log_file_action = rotate
```

Rationale

Automatically rotating logs (by setting this to rotate) minimizes the chances of the system unexpectedly running out of disk space by being overwhelmed with log data.

bash fix

```
var_auditd_max_log_file_action="rotate"

AUDITCONFIG=/etc/audit/auditd.conf

grep -q ^max_log_file_action $AUDITCONFIG && \
  sed -i 's/^max_log_file_action.*/max_log_file_action = '"$var_auditd_max_log_file_action"'/g'
$AUDITCONFIG
if ! [ $? -eq 0 ]; then
  echo "max_log_file_action = $var_auditd_max_log_file_action" >> $AUDITCONFIG
fi
```

NASA-ASCS-20040: Disable Core Dumps for All Users

NASA ASCS ID	NASA-ASCS-20040
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-010673

To disable core dumps for all users, add the following line to `/etc/security/limits.conf` :

```
*     hard   core    0
```

In cases that user notification of application crashes are not needed, consider also disabling ABRT service. Consult with OS distribution documnetation on how to disable ABRT properly. There is no security recommendation on disabling ABRT, simply a matter of administrator choice.

Rationale

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

bash fix

```
CONFIG_FILE=/etc/security/limits.conf
EXISTS_IF_REGEX="^.*\bhard\b.*\bcore\b.*"
SED_INLINE="s/^.*hard.*core.*$/*  hard  core  0/"
ECHO_APPEND="*  hard  core  0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i $SED_INLINE $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20043: Ensure Logrotate Runs Periodically

NASA ASCS ID	NASA-ASCS-20043
Severity	**Low**
Group	logging/system

The `logrotate` utility allows for the automatic rotation of log files. The frequency of rotation is specified in `/etc/logrotate.conf`, which triggers a cron task. To configure logrotate to run daily, add or correct the following line in `/etc/logrotate.conf`:

```
# rotate log files frequency
daily
```

Rationale

Log files that are not properly rotated run the risk of growing so large that they fill up the /var/log partition. Valuable logging information could be lost if the /var/log partition becomes full.

bash fix

```
LOGROTATE_CONF_FILE="/etc/logrotate.conf"
CRON_DAILY_LOGROTATE_FILE="/etc/cron.daily/logrotate"

# daily rotation is configured
grep -q "^daily$" $LOGROTATE_CONF_FILE|| echo "daily" >> $LOGROTATE_CONF_FILE

# remove any line configuring weekly, monthly or yearly rotations
sed -i -r "/^(weekly|monthly|yearly)$/d" $LOGROTATE_CONF_FILE

# configure cron.daily if not already
if ! grep -q "^[[:space:]]*/usr/sbin/logrotate[[:alnum:][:blank:][:punct:]]*$LOGROTATE_CONF_FILE$"
$CRON_DAILY_LOGROTATE_FILE; then
    echo "#!/bin/bash" > $CRON_DAILY_LOGROTATE_FILE
```

```
    echo "/usr/sbin/logrotate $LOGROTATE_CONF_FILE" >> $CRON_DAILY_LOGROTATE_FILE
fi
```

NASA-ASCS-20061: Disable Mounting of cramfs

NASA ASCS ID	NASA-ASCS-20061
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040025
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.1.1

The `cramfs` file system is designed to be simple and small, and to compress things well. It has a limit of 16MB file size and 256MB file system size. This makes it the choice for Internet of Things (IoT) and Industrial Control (IC) applications.

To configure the system to prevent the `cramfs` kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install cramfs /bin/true
```

This effectively prevents usage of this uncommon filesystem.

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system should be disabled.

bash fix

```
if grep --silent "^install cramfs" /etc/modprobe.d/cramfs.conf &> /dev/null
then
  sed -i "s/^install cramfs.*/install cramfs \/bin\/true/g" /etc/modprobe.d/cramfs.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/cramfs.conf
  echo "install cramfs /bin/true" >> /etc/modprobe.d/cramfs.conf
fi
```

NASA-ASCS-20062: Disable DCCP Support

NASA ASCS ID	NASA-ASCS-20062
Severity	**Low**
Group	network/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 3.1.3

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol, designed to support streaming media and telephony.

To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install dccp /bin/true
```

Rationale

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

bash fix

```
if grep --silent "^install dccp" /etc/modprobe.d/dccp.conf &> /dev/null
then
  sed -i 's/^install dccp.*/install dccp \/bin\/true/g' /etc/modprobe.d/dccp.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/dccp.conf
  echo "install dccp /bin/true" >> /etc/modprobe.d/dccp.conf
fi
```

NASA-ASCS-20063: Disable Mounting of freevxfs

NASA ASCS ID	NASA-ASCS-20063
Severity	**Low**
Group	permissions/system

The VERITAS File System (or VxFS; called JFS and OnlineJFS in HP-UX) is an extent-based file system. This file system is not a common file system used in Enterprise Linux.

Prevent usage of the uncommon filesystem `freevxfs`. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install freevxfs /bin/true
```

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system are better disabled.

bash fix

```
if grep --silent "^install freevxfs" /etc/modprobe.d/freevxfs.conf &> /dev/null
then
  sed -i 's/^install freevxfs.*/install freevxfs \/bin\/true/g' /etc/modprobe.d/freevxfs.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/freevxfs.conf
```

```
  echo "install freevxfs /bin/true" >> /etc/modprobe.d/freevxfs.conf
fi
```

NASA-ASCS-20064: Disable Mounting of hfs

NASA ASCS ID	NASA-ASCS-20064
Severity	**Low**
Group	permissions/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 1.1.1.2

Hierarchical File System (HFS) is a proprietary file system developed by Apple Inc. for use in computer systems running Mac OS.

Prevent the usage of the uncommon filesystem `hfs`. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install hfs /bin/true
```

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system shall be disabled.

bash fix

```
if grep --silent "^install hfs" /etc/modprobe.d/hfs.conf &> /dev/null
then
  sed -i 's/^install hfs.*/install hfs \/bin\/true/g' /etc/modprobe.d/hfs.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/hfs.conf
  echo "install hfs /bin/true" >> /etc/modprobe.d/hfs.conf
fi
```

NASA-ASCS-20065: Disable Mounting of hfsplus

NASA ASCS ID	NASA-ASCS-20065
Severity	**Low**
Group	permissions/system

HFS Plus or HFS+ (also known as Mac OS Extended or HFS Extended) is a journaling file system developed by Apple Inc.

Prevent the usage of the uncommon filesystem `hfsplus`. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install hfsplus /bin/true
```

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system should be disabled.

bash fix

```
if grep --silent "^install hfsplus" /etc/modprobe.d/hfsplus.conf &> /dev/null
then
  sed -i 's/^install hfsplus.*/install hfsplus \/bin\/true/g' /etc/modprobe.d/hfsplus.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/hfsplus.conf
  echo "install hfsplus /bin/true" >> /etc/modprobe.d/hfsplus.conf
fi
```

NASA-ASCS-20066: Disable Mounting of jffs2

NASA ASCS ID	NASA-ASCS-20066
Severity	**Low**
Group	permissions/system

Journalling Flash File System version 2 or JFFS2 is a log-structured file system for use with flash memory devices.

Prevent the usage of the uncommon filesystem `jffs2`. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install jffs2 /bin/true
```

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system shall be disabled.

bash fix

```
if grep --silent "^install jffs2" /etc/modprobe.d/jffs2.conf &> /dev/null
then
  sed -i 's/^install jffs2.*/install jffs2 \/bin\/true/g' /etc/modprobe.d/jffs2.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/jffs2.conf
  echo "install jffs2 /bin/true" >> /etc/modprobe.d/jffs2.conf
fi
```

NASA-ASCS-20067: Disable SCTP Support

NASA ASCS ID	NASA-ASCS-20067
Severity	**Low**
Group	network/system
STIG Reference	RHEL_8_STIG RHEL-08-040023
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 3.1.2

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol designed to support the idea of message-oriented communication with several streams of messages within one connection. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install sctp /bin/true
```

Rationale

Disabling SCTP protects the system against exploitation of any flaws in its implementation.

bash fix

```
if grep --silent "^install sctp" /etc/modprobe.d/sctp.conf &> /dev/null
then
  sed -i 's/^install sctp.*/install sctp \/bin\/true/g' /etc/modprobe.d/sctp.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/sctp.conf
  echo "install sctp /bin/true" >> /etc/modprobe.d/sctp.conf
fi
```

NASA-ASCS-20068: Disable Mounting of squashfs

NASA ASCS ID	NASA-ASCS-20068
Severity	**Low**
Group	permissions/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 1.1.1.2

Prevent the usage of the uncommon filesystem `squashfs`. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install squashfs /bin/true
```

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system shall be disabled.

bash fix

```
if grep --silent "^install squashfs" /etc/modprobe.d/squashfs.conf &> /dev/null
then
  sed -i 's/^install squashfs.*/install squashfs \/bin\/true/g' /etc/modprobe.d/squashfs.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/squashfs.conf
  echo "install squashfs /bin/true" >> /etc/modprobe.d/squashfs.conf
fi
```

NASA-ASCS-20069: Disable Mounting of udf

NASA ASCS ID	NASA-ASCS-20069
Severity	**Low**
Group	permissions/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 1.1.1.3

Universal Disk Format (UDF) is an open, vendor-neutral file system for computer data storage for a broad range of media.

Prevent the usage of the uncommon filesystem `udf`. To configure the system to prevent the kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install udf /bin/true
```

Rationale

Linux kernel modules which implement filesystems that are not needed by the local system shall be disabled.

bash fix

```
if grep --silent "^install udf" /etc/modprobe.d/udf.conf &> /dev/null
then
  sed -i 's/^install udf.*/install udf \/bin\/true/g' /etc/modprobe.d/udf.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/udf.conf
  echo "install udf /bin/true" >> /etc/modprobe.d/udf.conf
fi
```

NASA-ASCS-20071: Add nodev Option to /dev/shm

NASA ASCS ID	NASA-ASCS-20071
Severity	**Low**

Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040120
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.8.1
MITRE D3FEND Reference	D3-LFP

The `nodev` mount option can be used to prevent creation of device files in `/dev/shm` . Legitimate character and block devices should not exist within temporary directories like `/dev/shm` . Add the `nodev` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/dev/shm` .

Rationale

The only legitimate location for device files is the /dev directory located on the root partition. The only exception to this is chroot jails.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /dev/shm )" ]]
then
  if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /dev/shm | grep -v nodev )" ]]
  then
    sed -r -i "s/^([a-Z0-9_\-]*)\s+(\/dev\/shm)\s+([a-Z0-9]*)\s+([a-Z0-9,=_\-]*)\s+([0-9]*)\s+([0-
9]*)(\s+)?$/\1  \2  \3  \4,nodev  \5 \6/" $FSTAB_FILE
  fi
else
  printf "tmpfs    /dev/shm    tmpfs         defaults,noexec,nodev,nosuid    0 0\n" >> /etc/fstab
fi
```

NASA-ASCS-20072: Add noexec Option to /dev/shm

NASA ASCS ID	NASA-ASCS-20072
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040122
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.8.2
MITRE ATT&CK Reference	T1059, T1564, TA0002
MITRE D3FEND Reference	D3-LFP

The `noexec` mount option can be used to prevent binaries from being executed out of `/dev/shm` . It can be dangerous to allow the execution of binaries from world-writable temporary storage directories such as `/dev/shm` . Add the `noexec` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/dev/shm` .

Rationale

Allowing users to execute binaries from world-writable directories such as /dev/shm can expose the system to compromise.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /dev/shm )" ]]
then
  if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /dev/shm | grep -v noexec )" ]]
  then
    sed -r -i "s/^([a-Z0-9_\-]*)\s+(\/dev\/shm)\s+([a-Z0-9]*)\s+([a-Z0-9,=_\-]*)\s+([0-9]*)\s+([0-
9]*)(\s+)?$/\1  \2  \3  \4,noexec  \5 \6/" $FSTAB_FILE
  fi
else
  printf "tmpfs    /dev/shm    tmpfs         defaults,noexec,nodev,nosuid    0 0\n" >> /etc/fstab
fi
```

NASA-ASCS-20073: Add nosuid Option to /dev/shm

NASA ASCS ID	NASA-ASCS-20073
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040121
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.8.3
MITRE ATT&CK Reference	T1548.001, M1028
MITRE D3FEND Reference	D3-LFP

The `nosuid` mount option can be used to prevent execution of setuid programs in `/dev/shm` . The SUID and SGID permissions should not be required in these world-writable directories. Add the `nosuid` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/dev/shm` .

Rationale

SUID and SGID executables should be tightly controlled. Users should not be able to execute SUID or SGID binaries from temporary storage partitions.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /dev/shm )" ]]
then
  if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /dev/shm | grep -v nosuid )" ]]
  then
```

```
    sed -r -i "s/^([a-Z0-9_\-]*)\s+(\/dev\/shm)\s+([a-Z0-9]*)\s+([a-Z0-9,=_\-]*)\s+([0-9]*)\s+([0-
9]*)(\s+)?$/\1  \2  \3  \4,nosuid  \5 \6/" $FSTAB_FILE
  fi
else
  printf "tmpfs    /dev/shm    tmpfs         defaults,noexec,nodev,nosuid    0 0\n" >> /etc/fstab
fi
```

NASA-ASCS-20074: Add nodev Option to Non-Root Local Partitions

NASA ASCS ID	NASA-ASCS-20074
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-010580
MITRE D3FEND Reference	D3-LFP

The `nodev` mount option prevents files from being interpreted as character or block devices. Legitimate character and block devices should exist only in the `/dev` directory on the root partition or within chroot jails built for system services. Add the `nodev` option to the fourth column of `/etc/fstab` for the line which controls mounting of any non-root local partitions.

Rationale

The nodev mount option prevents files from being interpreted as character or block devices. The only legitimate location for device files is the /dev directory located on the root partition. The only exceptions to this are chroot jails, and nodev shall not be set on these filesystems.

NASA-ASCS-20075: Mount Remote Filesystems with nodev

NASA ASCS ID	NASA-ASCS-20075
Severity	**Low**
Group	nfs_and_rpc/services
STIG Reference	RHEL_8_STIG RHEL-08-010640
MITRE D3FEND Reference	D3-LFP

Add the `nodev` option to the fourth column of `/etc/fstab` for the line which controls mounting of any Network File System (NFS) mounts.

Rationale

Legitimate device files should only exist in the /dev directory. Network File System (NFS) mounts should not present device files to users.

NASA-ASCS-20076: Add nodev Option to /tmp

NASA ASCS ID	NASA-ASCS-20076
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040123
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.2.2
MITRE D3FEND Reference	D3-LFP

The `nodev` mount option can be used to prevent device files from being created in `/tmp` . Legitimate character and block devices should not exist within temporary directories like `/tmp` . Add the `nodev` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/tmp` .

Rationale

The only legitimate location for device files is the /dev directory located on the root partition. The only exceptions to this are chroot jails.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /tmp | grep -v nodev )" ]]
then
  sed -r -i "s/^(.*)\s+(\/tmp)\s+(.*)\s+(.*)\s+(.*)\s+(.*)$/\1\t\2\t\3\t\4,nodev \5 \6/"
$FSTAB_FILE
fi
```

NASA-ASCS-20077: Add noexec Option to /tmp

NASA ASCS ID	NASA-ASCS-20077
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040125
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.2.3
MITRE ATT&CK Reference	T1059, T1564, TA0002
MITRE D3FEND Reference	D3-LFP

The `noexec` mount option can be used to prevent binaries from being executed out of `/tmp` . Add the `noexec` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/tmp` .

The `apt` configuration has a known issue with `noexec` being used on `/tmp`.

What you might see:

```
The following NEW packages will be installed
  bind9
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0B/255kB of archives.
After this operation, 778kB of additional disk space will be used.
Preconfiguring packages ...
Can't exec "/var/tmp/bind9.config.326141": Permission denied at
/usr/share/perl/5.10/IPC/Open3.pm line 168.
open2: exec of /var/tmp/bind9.config.326141 configure  failed at
/usr/share/perl5/Debconf/ConfModule.pm line 59
bind9 failed to preconfigure, with exit status 255
```

This can be overcome by changing the configuration to a different location (permissions confined to `_apt`) and updated in `/etc/apt.conf.d/`.

`/etc/apt.conf.d/tmpchange.conf`

```
APT
{
  ExtractTemplates
  {
    TempDir "/var/local/apt_tmp";
  };
};
```

Rationale

Allowing users to execute binaries from world-writable directories such as /tmp should never be necessary in normal operation and can expose the system to potential compromise.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /tmp | grep -v noexec )" ]]
then
  sed -r -i "s/^(.*)\s+(\/tmp)\s+(.*)\s+(.*)\s+(.*)\s+(.*)$/\1\t\2\t\3\t\4,noexec \5 \6/"
$FSTAB_FILE
fi
```

NASA-ASCS-20078: Add nosuid Option to /tmp

NASA ASCS ID	NASA-ASCS-20078
Severity	**Low**

Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040124
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.2.4
MITRE ATT&CK Reference	T1548.001, M1028
MITRE D3FEND Reference	D3-LFP

The `nosuid` mount option can be used to prevent execution of setuid programs in `/tmp` . The SUID and SGID permissions should not be required in these world-writable directories. Add the `nosuid` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/tmp` .

Rationale

The presence of SUID and SGID executables should be tightly controlled. Users should not be able to execute SUID or SGID binaries from temporary storage partitions.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /tmp | grep -v nosuid )" ]]
then
  sed -r -i "s/^(.*)\s+(\/tmp)\s+(.*)\s+(.*)\s+(.*)\s+(.*)$/\1\t\2\t\3\t\4,nosuid \5 \6/"
$FSTAB_FILE
fi
```

NASA-ASCS-20079: Add nodev Option to /var/tmp

NASA ASCS ID	NASA-ASCS-20079
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040132
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.4.4
MITRE D3FEND Reference	D3-LFP

The `nodev` mount option can be used to prevent device files from being created in `/var/tmp` . Legitimate character and block devices should not exist within temporary directories like `/var/tmp` . Add the `nodev` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/var/tmp` .

Rationale

The only legitimate location for device files is the /dev directory located on the root partition. The only exceptions to this are chroot jails.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /var/tmp | grep -v nodev )" ]]
then
  sed -r -i "s/^(.*)\s+(\/var\/tmp)\s+(.*)\s+(.*)\s+(.*)$/\1\t\2\t\3\t\4,nodev \5 \6/"
$FSTAB_FILE
fi
```

NASA-ASCS-20080: Add nosuid Option to /var/tmp

NASA ASCS ID	NASA-ASCS-20080
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040133
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.4.3
MITRE ATT&CK Reference	T1548.001, M1028
MITRE D3FEND Reference	D3-LFP

The `nosuid` mount option can be used to prevent execution of setuid programs in `/var/tmp` . The SUID and SGID permissions should not be required in these world-writable directories. Add the `nosuid` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/var/tmp` .

Rationale

The presence of SUID and SGID executables should be tightly controlled. Users should not be able to execute SUID or SGID binaries from temporary storage partitions.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /var/tmp | grep -v nosuid )" ]]
then
  sed -r -i "s/^(.*)\s+(\/var\/tmp)\s+(.*)\s+(.*)\s+(.*)$/\1\t\2\t\3\t\4,nosuid \5 \6/"
$FSTAB_FILE
fi
```

NASA-ASCS-20082: Remove Rsh Trust Files

NASA ASCS ID	NASA-ASCS-20082
Severity	**Low**

Group	obsolete/services

The files `/etc/hosts.equiv` and `~/.rhosts` (in each user's home directory) list remote hosts and users that are trusted by the local system when using the rshd daemon. To remove these files, run the following command to delete them from any location:

```
$ rm /etc/hosts.equiv
```

```
$ rm ~/.rhosts
```

Rationale

Trust files are convenient, but when used in conjunction with the R-services, they can allow unauthenticated access to a system.

bash fix

```
find /home -maxdepth 2 -type f -name .rhosts -exec rm -f '{}' \;
rm -f /etc/hosts.equiv
```

NASA-ASCS-20086: Remove tftp Daemon

NASA ASCS ID	NASA-ASCS-20086
Severity	**Low**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-040190
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 2.2.9
MITRE ATT&CK Reference	TA0008, T1210, M1042

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol, typically used to automatically transfer configuration or boot files between systems. The protocol does not support authentication and can be exploited easily.

On a Linux system, the package `tftp` is a client program that allows for connections to a `tftp` server.

To remove the `tftp` client from systems use:

```
yum remove tftp
```

```
apt-get purge tftp
```

```
zypper remove tftp
```

Or other package manager to remove the `tftp` client from the system.

Rationale

TFTP shall be removed unless there is a specific need for TFTP (such as a boot server). In those cases, use extreme caution when configuring the services.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q tftp &> /dev/null
  then
    yum -y remove tftp &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' tftp )" == "installed" ]]
  then
    apt-get -y purge tftp &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q tftp &> /dev/null
  then
    zypper --non-interactive remove tftp &> /dev/null
  fi
fi
```

NASA-ASCS-20087: Uninstall xinetd Package

NASA ASCS ID	NASA-ASCS-20087
Severity	**Low**
Group	obsolete/services
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 2.2.1
MITRE ATT&CK Reference	TA0008, T1210, M1042, TA0004, T1068

The Extended Internet Service Daemon (`xinetd`) is a super-server daemon which runs other server daemons like `tftpd`, `imapd` and `telnetd`. The `xinetd` service is rarely needed on standard Linux installations.

The `xinetd` package is removed with the following command:

```
yum remove xinetd
```

or

```
apt-get purge xinetd
```

or

```
zypper remove xinetd
```

Rationale

Removing the xinetd package decreases the risk of the xinetd services being accidentally (or intentionally) activated.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q xinetd &> /dev/null
  then
    yum -y remove xinetd &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' xinetd )" == "installed" ]]
  then
    apt-get -y purge xinetd &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q xinetd &> /dev/null
  then
    zypper --non-interactive remove xinetd &> /dev/null
  fi
fi
```

NASA-ASCS-20088: Ensure /var/log Located On Separate Partition

NASA ASCS ID	NASA-ASCS-20088
Severity	**Low**
Group	software/system
STIG Reference	RHEL_8_STIG RHEL-08-010541, RHEL_8_STIG RHEL-08-030660
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 1.1.5.1

System logs are stored in the `/var/log` directory. The `/vat/log` mount shall have its own partition or logical volume at installation time, or migrate it using LVM.

Rationale

Placing /var/log in its own partition enables better separation between log files and other files in /var/.

NASA-ASCS-20089: Ensure /var/log/audit Located On Separate Partition

NASA ASCS ID	NASA-ASCS-20089
Severity	**Low**
Group	software/system
NIST SP 800-53r5 Reference	AU-09
STIG Reference	RHEL_8_STIG RHEL-08-010542, RHEL_8_STIG RHEL-08-030660
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 1.1.6.1

Audit logs are stored in the `/var/log/audit` directory. The `/var/log/audit` mount shall have its own partition or logical volume at installation time, or migrate it later using LVM. Make absolutely certain that it is large enough to store all audit logs that will be created by the auditing daemon.

Rationale

Placing /var/log/audit in its own partition enables better separation between audit files and other files and helps ensure that auditing cannot be halted due to the partition running out of space.

NASA-ASCS-20090: Ensure /var/tmp Located On Separate Partition

NASA ASCS ID	NASA-ASCS-20090
Severity	**Low**
Group	software/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 1.1.4.1

The `/var/tmp` directory is a world-writable directory used for temporary file storage. The `/var/tmp` mount shall have its own partition or logical volume at installation time, or migrate it using Logical Volume Managemer (LVM).

Rationale

The /var/tmp partition is used as temporary storage by many programs. Placing /var/tmp in its own partition enables the setting of more restrictive mount options, which can help protect programs that use it.

NASA-ASCS-20092: Ensure the root User PATH Variable Does Not Include Relative Paths or Null Directories

NASA ASCS ID	NASA-ASCS-20092
Severity	**Low**
Group	accounts/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.7
MITRE ATT&CK Reference	T1574

Ensure that none of the directories in root's path:

- Are equal to a single `.` character.
- Contain any instances that lead to relative path traversal, such as `..` or beginning a path without the slash (`/`) character.
- Use "empty" elements in the path (which behave the same as a single `.` character). Examples: `PATH=:/bin` or `PATH=/bin:` or `PATH=/bin::/sbin`

Rationale

Including these entries increases the risk that root could execute code from an untrusted location.

NASA-ASCS-20108: Disable Core Dumps for SUID programs

NASA ASCS ID	NASA-ASCS-20108
Severity	**Low**
Group	permissions/system
MITRE ATT&CK Reference	TA0007, T1083, T1005
Control Setting	0

To set the runtime status of the `fs.suid_dumpable` kernel parameter, run the following command:

```
$ sysctl -w fs.suid_dumpable=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
fs.suid_dumpable = 0
```

Rationale

The core dump of a setuid program is more likely to contain sensitive data, as the program itself runs with greater privileges than the user who initiated execution of the program. Disabling the ability for any setuid program to write a

core file decreases the risk of unauthorized access of such data.

bash fix

```
# Set runtime for fs.suid_dumpable
/sbin/sysctl -q -n -w fs.suid_dumpable=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^fs.suid_dumpable"
SED_INLINE="s/^fs.suid_dumpable.*$/fs.suid_dumpable=0/"
ECHO_APPEND="fs.suid_dumpable=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20110: Enable Kernel Parameter to Log Martian Packets

NASA ASCS ID	NASA-ASCS-20110
Severity	**Low**
Group	network/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.4
MITRE ATT&CK Reference	T1557, T1498
Control Setting	1

To set the runtime status of the `net.ipv4.conf.all.log_martians` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.all.log_martians=1
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.all.log_martians = 1
```

Rationale

The presence of martian packets (which have impossible addresses) as well as spoofed packets, source-routed packets, and redirects, could be a sign of nefarious network activity. Logging these packets enables this activity to be detected.

bash fix

```
# Set runtime for net.ipv4.conf.all.log_martians
/sbin/sysctl -q -n -w net.ipv4.conf.all.log_martians=1

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.all.log_martians"
SED_INLINE="s/^net.ipv4.conf.all.log_martians.*$/net.ipv4.conf.all.log_martians=1/"
ECHO_APPEND="net.ipv4.conf.all.log_martians=1"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20111: Enable Kernel Parameter to Use Reverse Path Filtering for All Interfaces

NASA ASCS ID	NASA-ASCS-20111
Severity	**Low**
Group	network/system
STIG Reference	RHEL_8_STIG RHEL-08-040285
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.7
MITRE ATT&CK Reference	T1557, T1498
Control Setting	1

The `rp_filter` kernel parameter will drop packages with improper addresses (such as 10.0.0.0/8 on internet facing interface). Improper network attempts can indicate spoofing.

To set the runtime status of the `net.ipv4.conf.all.rp_filter` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.all.rp_filter=1
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.all.rp_filter = 1
```

Rationale

Enabling reverse path filtering drops packets with source addresses that should not have been able to be received on the interface where they were received. It should not be used on systems which are routers for complicated

networks but is helpful for end hosts and routers serving small networks.

bash fix

```
# Set runtime for net.ipv4.conf.all.rp_filter
/sbin/sysctl -q -n -w net.ipv4.conf.all.rp_filter=1

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.all.rp_filter"
SED_INLINE="s/^net.ipv4.conf.all.rp_filter.*$/net.ipv4.conf.all.rp_filter=1/"
ECHO_APPEND="net.ipv4.conf.all.rp_filter=1"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20112: Disable Kernel Parameter for Accepting Secure Redirects for All Interfaces

NASA ASCS ID	NASA-ASCS-20112
Severity	**Low**
Group	network/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.3
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

Prevents hijacking of routing path by only allowing redirects from gateways known in our routing table.

Ubuntu recommendation is `1`, CIS recommends `0`.

To set the runtime status of the `net.ipv4.conf.all.secure_redirects` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.all.secure_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.all.secure_redirects = 0
```

Rationale

Accepting secure ICMP redirects (from those gateways listed as default gateways) does not ensure protection from compromised gateways.

bash fix

```
# Set runtime for net.ipv4.conf.all.secure_redirects
/sbin/sysctl -q -n -w net.ipv4.conf.all.secure_redirects=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.all.secure_redirects"
SED_INLINE="s/^net.ipv4.conf.all.secure_redirects.*$/net.ipv4.conf.all.secure_redirects=0/"
ECHO_APPEND="net.ipv4.conf.all.secure_redirects=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20113: Enable Kernel Parameter to Use Reverse Path Filtering by Default

NASA ASCS ID	NASA-ASCS-20113
Severity	**Low**
Group	network/system
STIG Reference	RHEL_8_STIG RHEL-08-040285
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.7
MITRE ATT&CK Reference	T1557, T1498
Control Setting	1

To set the runtime status of the `net.ipv4.conf.default.rp_filter` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.default.rp_filter=1
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.default.rp_filter = 1
```

Rationale

Enabling reverse path filtering drops packets with source addresses that should not have been able to be received on the interface where they were received. It should not be used on systems which are routers for complicated

networks but is helpful for end hosts and routers serving small networks.

bash fix

```
# Set runtime for net.ipv4.conf.default.rp_filter
/sbin/sysctl -q -n -w net.ipv4.conf.default.rp_filter=1

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.default.rp_filter"
SED_INLINE="s/^net.ipv4.conf.default.rp_filter.*$/net.ipv4.conf.default.rp_filter=1/"
ECHO_APPEND="net.ipv4.conf.default.rp_filter=1"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20114: Disable Kernel Parameter for Accepting Secure Redirects By Default

NASA ASCS ID	NASA-ASCS-20114
Severity	**Low**
Group	network/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.3
MITRE ATT&CK Reference	T1557, T1565, M1042
Control Setting	0

To set the runtime status of the `net.ipv4.conf.default.secure_redirects` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.conf.default.secure_redirects=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.conf.default.secure_redirects = 0
```

Rationale

Accepting secure ICMP redirects (from those gateways listed as default gateways) has few legitimate uses. It should be disabled unless it is absolutely required.

bash fix

```
/sbin/sysctl -q -n -w net.ipv4.conf.default.secure_redirects=0

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.conf.default.secure_redirects"
SED_INLINE="s/^net.ipv4.conf.default.secure_redirects.*$/net.ipv4.conf.default.secure_redirects=0/"
ECHO_APPEND="net.ipv4.conf.default.secure_redirects=0"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20115: Enable Kernel Parameter to Ignore Bogus ICMP Error Responses

NASA ASCS ID	NASA-ASCS-20115
Severity	**Low**
Group	network/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.6
MITRE ATT&CK Reference	T0814
Control Setting	1

Some routers ignore RFC 1122 and send junk error responses that get logged. It may be possible to trigger this logging by spoofing; this would lead to filling up the hard disk with junk logs, causing a denial of service.

To set the runtime status of the `net.ipv4.icmp_ignore_bogus_error_responses` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Rationale

Ignoring bogus ICMP error responses reduces log size.

bash fix

```
# Set runtime for net.ipv4.icmp_ignore_bogus_error_responses
/sbin/sysctl -q -n -w net.ipv4.icmp_ignore_bogus_error_responses=1

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.icmp_ignore_bogus_error_responses"
SED_INLINE="s/^net.ipv4.icmp_ignore_bogus_error_responses.*$/net.ipv4.icmp_ignore_bogus_error_respo
nses=1/"
ECHO_APPEND="net.ipv4.icmp_ignore_bogus_error_responses=1"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20116: Enable Kernel Parameter to Use TCP Syncookies

NASA ASCS ID	NASA-ASCS-20116
Severity	**Low**
Group	network/system
NIST SP 800-53r5 Reference	SC-05 (2)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 3.3.8
MITRE ATT&CK Reference	T0814
Control Setting	1

To set the runtime status of the `net.ipv4.tcp_syncookies` kernel parameter, run the following command:

```
$ sysctl -w net.ipv4.tcp_syncookies=1
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv4.tcp_syncookies = 1
```

Rationale

A TCP SYN flood attack can cause a denial of service by filling a system's TCP connection table with connections in the SYN_RCVD state. Syncookies can be used to track a connection when a subsequent ACK is received, by verifying the initiator is attempting a valid connection and is not a flood source. This feature is activated when a flood condition is detected and enables the system to continue servicing valid connection requests.

bash fix

```
# Set runtime for net.ipv4.tcp_syncookies
/sbin/sysctl -q -n -w net.ipv4.tcp_syncookies=1

CONFIG_FILE=/etc/sysctl.conf
EXISTS_IF_REGEX="^net.ipv4.tcp_syncookies"
SED_INLINE="s/^net.ipv4.tcp_syncookies.*$/net.ipv4.tcp_syncookies=1/"
ECHO_APPEND="net.ipv4.tcp_syncookies=1"

if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
then
  sed -i "$SED_INLINE" $CONFIG_FILE
else
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-20117: Disable Accepting IPv6 Router Advertisements

NASA ASCS ID	NASA-ASCS-20117
Severity	**Low**
Group	network/system
STIG Reference	RHEL_8_STIG RHEL-08-040261
Control Setting	0

To set the runtime status of the `net.ipv6.conf.all.accept_ra` kernel parameter, run the following command:

```
$ sysctl -w net.ipv6.conf.all.accept_ra=0
```

If this is not the system's default value, add the following line to `/etc/sysctl.conf` :

```
net.ipv6.conf.all.accept_ra = 0
```

Rationale

An illicit router advertisement message could result in a man-in-the-middle attack.

bash fix

```
DISABLED=$(</sys/module/ipv6/parameters/disable)
if [[ "$DISABLED" == "0" ]]
then
  # Set runtime for net.ipv6.conf.all.accept_ra
  /sbin/sysctl -q -n -w net.ipv6.conf.all.accept_ra=0
```

```
  CONFIG_FILE=/etc/sysctl.conf
  EXISTS_IF_REGEX="^net.ipv6.conf.all.accept_ra"
  SED_INLINE="s/^net.ipv6.conf.all.accept_ra.*$/net.ipv6.conf.all.accept_ra=0/"
  ECHO_APPEND="net.ipv6.conf.all.accept_ra=0"

  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i "$SED_INLINE" $CONFIG_FILE
  else
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-20153: Ensure yum removes unneeded dependencies

NASA ASCS ID	NASA-ASCS-20153
Severity	**Low**
Group	software/system
STIG Reference	RHEL_8_STIG RHEL-08-010440

The `yum` utility shall be configured to remove previous software components after updates have been installed.

To configure `yum` to remove the previous software components after updating, set the `clean_requirements_on_remove` to `1` in `/etc/yum.conf`.

Rationale

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by some malicious actors.

bash fix

```
if which yum &> /dev/null
then
  if grep --silent ^clean_requirements_on_remove /etc/yum.conf ; then
    sed -i "s/^clean_requirements_on_remove.*/clean_requirements_on_remove=1/g" /etc/yum.conf
  else
    echo -e "\n# Set clean_requirements_on_remove to 1 per security requirements" >> /etc/yum.conf
    echo "clean_requirements_on_remove=1" >> /etc/yum.conf
  fi
fi
```

NASA-ASCS-20156: Set Last Logon/Access Notification

NASA ASCS ID	NASA-ASCS-20156

Severity	**Low**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-09
STIG Reference	RHEL_8_STIG RHEL-08-020340
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.3.12
MITRE ATT&CK Reference	DS0028

To configure the system to notify users of last logon/access using `pam_lastlog` , add or correct the `pam_lastlog` settings in `/etc/pam.d/postlogin` to read as follows:

```
session     [success=1 default=ignore] pam_succeed_if.so service !~ gdm* service !~ su* quiet
session     [default=1]   pam_lastlog.so nowtmp showfailed
session     optional      pam_lastlog.so silent noupdate showfailed
```

Modern distributions utilize tools that modify PAM files, in order to ensure any modification of configurations in `/etc/pam.d/` consider using the distribution prescribed method for maintaining PAM configurations. In RHEL 8 the use of `authselect` and in Ubuntu 18.04+ the use of `pam-auth-update`. Refer to distribution documentation for appropriate configuration use. The PIV-SSSD Handbook has both `authselect` and `pam-auth-update` content that can also help.

Rationale

Users need to be aware of activity that occurs regarding their account. Providing users with information regarding the number of unsuccessful attempts that were made to log in to their account allows the user to determine if any unauthorized activity has occurred and gives them an opportunity to notify administrators.

bash fix

```
# NOTE: Use of authselect tool requires System Administrator to fix. See note in specification
document.
```

NASA-ASCS-20159: Verify that Shared Library Files Have Root Ownership

NASA ASCS ID	NASA-ASCS-20159
Severity	**Low**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
STIG Reference	RHEL_8_STIG RHEL-08-010340

MITRE ATT&CK Reference	T1083, M1022
MITRE D3FEND Reference	D3-LFP

System-wide shared library files, which are linked to executables during process load time or run time, are stored in the following directories by default:

```
/lib
/lib64
/usr/lib
/usr/lib64
```

Kernel modules, which can be added to the kernel during runtime, are also stored in `/lib/modules` . All files in these directories should be owned by the `root` user. If the directory, or any file in these directories, is found to be owned by a user other than root, correct its ownership with the following command:

```
$ chown root FILE
```

Rationale

Files from shared library directories are loaded into the address space of processes (including privileged ones) or of the kernel itself at runtime. Proper ownership is necessary to protect the integrity of the system.

bash fix

```
for LIBDIR in /usr/lib /usr/lib64 /lib /lib64
do
  if [ -d $LIBDIR ]
  then
    find -L $LIBDIR \! -user root -exec chown root {} \;
  fi
done
```

NASA-ASCS-20161: Ensure that User Home Directories are not Group-Writable or World-Readable

NASA ASCS ID	NASA-ASCS-20161
Severity	**Low**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-03 (4)
STIG Reference	RHEL_8_STIG RHEL-08-010750, RHEL_8_STIG RHEL-08-010731, RHEL_8_STIG RHEL-08-010730

CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.11
MITRE ATT&CK Reference	T1083, M1022
MITRE D3FEND Reference	D3-LFP

Confirm the appropriate user permissions exist within the user home directory:

```
# ls -ld /home/USER
```

NOTE:To confirm that a user is valid we are checking if `USER` is in `/etc/passwd`, has a valid shell described in `/etc/shells`, and does not have a `/sbin/nologin` shell.

Ensure that the directory is not group-writable and that it is not world-readable. If necessary, repair the permissions:

```
# chmod g-w /home/USER
# chmod o-rwx /home/USER
```

Rationale

User home directories contain many configuration files which affect the behavior of a user's account. No user shall have write permission to another user's home directory. Group shared directories can be configured in sub-directories or elsewhere in the filesystem if they are needed. User home directories shall not be world-readable, as it would disclose file names to other users. If a subset of users need read access to one another's home directories, this can be provided using groups or Access Control Lists (ACLs).

NASA-ASCS-20163: Mount Remote Filesystems with nosuid

NASA ASCS ID	NASA-ASCS-20163
Severity	**Low**
Group	nfs_and_rpc/services
STIG Reference	RHEL_8_STIG RHEL-08-010650
MITRE ATT&CK Reference	T1548.001, M1028

Add the `nosuid` option to the fourth column of `/etc/fstab` for the line which controls mounting of any NFS mounts.

Rationale

NFS mounts should not present suid binaries to users. Only vendor-supplied suid executables should be installed to their default location on the local filesystem.

NASA-ASCS-20171: Ensure /tmp Located On Separate Partition

NASA ASCS ID	NASA-ASCS-20171
Severity	**Low**
Group	software/system
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.2.1

The `/tmp` directory is a world-writable directory used for temporary file storage. The `/tmp` mount shall have its own partition or logical volume at installation time, or migrate it using LVM.

Rationale

The /tmp partition is used as temporary storage by many programs. Placing /tmp in its own partition enables the setting of more restrictive mount options, which can help protect programs that use it.

NASA-ASCS-20172: Ensure No Device Files are Unlabeled by SELinux

NASA ASCS ID	NASA-ASCS-20172
Severity	**Low**
Group	mandatory_access_control
NIST SP 800-53r5 Reference	AC-03 (3)

Ensure system device files, which are used for communication with important system resources, are labeled with proper SELinux types.

To check for unlabeled device files, run the following command:

```
#> find /dev -context *:device_t:* \( -type c -o -type b \) -printf "%p %Z\n"
```

It should produce no output in most systems, however there are known devices that can not be labeled. Labels for known devices are excluded in the control.

If device is found unlabeled, and it is capable of being labeled properly, use the following command:

Example of /dev/vhost-vsock

```
chcon -t vhost_device_t /dev/vhost-vsock
semanage fcontext -a -t vhost_device_t /dev/vhost-vsock
```

If `kdump` is enabled for development purposes the `/dev/kdump0` and `/dev/trace0` will be unlabeled, control NASA-ASCS-20176. While these devices are going to be excluded from the device label scanning, it is up to the system administrator to know that unlabeled devices will not have restrictions as other devices will and should be monitored in other ways outside of SELinux labels.

Additional known device labels which are excluded and should be monitored by the System Administrator using other tools:

- dell-smbios
- sisap0, sisevt0 ((SEP)
- zfs
- kdump0 and trace0 (kdump, see above admonition)
- hypercall, privcmd, xenbus_backend (on Xen hypervisors)
- ss0 and mmpmem0 (GPFS cluster file system nodes)
- sep5, pax, socperf3 (Intel vtune)

Items in the exclude list are gathered from the NASA community of System Administrators and ISOs and reviewed prior to being added. If you find items that are not able to be labeled, please contact ASCS to ensure we provide an appropriate list of excluded devices.

Rationale

If a device file carries the SELinux type device_t, then SELinux cannot properly restrict access to the device file.

NASA-ASCS-20176: Disable KDump Kernel Crash Analyzer (kdump)

NASA ASCS ID	NASA-ASCS-20176
Severity	**Low**
Group	base/services
STIG Reference	RHEL_8_STIG RHEL-08-010670

The `kdump` service provides a kernel crash dump analyzer. It uses the `kexec` system call to boot a secondary kernel ("capture" kernel) following a system crash, which can load information from the crashed kernel for analysis. The `kdump` service shall be disabled with the following command:

```
$ systemctl disable kdump.service
```

Using `kdump` for development purposes will introduce unlabeled devices. In NASA-ASCS-20172, the control for device label context in SELinux systems, makes note that care should be taken to consider managing unlabeled devices `/dev/kdump0` and `/dev/trace0`.

Rationale

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps 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. Unless the system is used for kernel development or testing, there is little need to run the kdump service.

bash fix

```
if which systemctl &> /dev/null
then
  SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?kdump(d)?\.service" | sed "s/^\s\+//" |
cut -d" " -f1 )
  if systemctl is-active $SERVICE &> /dev/null
  then
    systemctl stop $SERVICE &> /dev/null
  fi
  if systemctl is-enabled $SERVICE &> /dev/null
  then
    systemctl disable $SERVICE &> /dev/null
  fi
else
  SERVICE=$( chkconfig | grep "^kdump" | cut -d" " -f1 )
  chkconfig $SERVICE off &> /dev/null
  service $SERVICE stop &> /dev/null
fi
```

NASA-ASCS-20198: Ensure All SGID Executables Are Authorized

NASA ASCS ID	NASA-ASCS-20198
Severity	**Low**
Group	permissions/system

The SGID (set group id) bit should be set only on files that were installed via authorized means. A straightforward means of identifying unauthorized SGID files is determine if any were not installed as part of an RPM package, which is cryptographically verified. Investigate the origin of any unpackaged SGID files.

Rationale

Executable files with the SGID permission run with the privileges of the owner of the file. SGID files of uncertain provenance could allow for unprivileged users to elevate privileges. The presence of these files should be strictly controlled on the system.

NASA-ASCS-20199: Ensure All SUID Executables Are Authorized

NASA ASCS ID	NASA-ASCS-20199
Severity	**Low**
Group	permissions/system

The SUID (set user id) bit should be set only on files that were installed via authorized means. A straightforward means of identifying unauthorized SGID files is determine if any were not installed as part of an RPM package, which is cryptographically verified. Investigate the origin of any unpackaged SUID files.

Rationale

Executable files with the SUID permission run with the privileges of the owner of the file. SUID files of uncertain provenance could allow for unprivileged users to elevate privileges. The presence of these files should be strictly controlled on the system.

NASA-ASCS-20210: Disable RDS Support

NASA ASCS ID	NASA-ASCS-20210
Severity	**Low**
Group	network/system
NIST SP 800-53r5 Reference	SC-08
STIG Reference	RHEL_8_STIG RHEL-08-040111

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide reliable, high-bandwidth, low-latency communications between nodes in a cluster. To configure the system to prevent the `rds` kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install rds /bin/true
```

Rationale

Disabling RDS protects the system against exploitation of any flaws in its implementation.

NASA-ASCS-20211: Disable TIPC Support

NASA ASCS ID	NASA-ASCS-20211
Severity	**Low**
Group	network/system
STIG Reference	RHEL_8_STIG RHEL-08-040024

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communications between nodes in a cluster. To configure the system to prevent the `tipc` kernel module from being loaded, add the following line to a file in the directory `/etc/modprobe.d` :

```
install tipc /bin/true
```

Rationale

Disabling TIPC protects the system against exploitation of any flaws in its implementation.

bash fix

```
if grep --silent "^install tipc" /etc/modprobe.d/tipc.conf
then
  sed -i "s/^install tipc.*/install tipc \/bin\/true/g" /etc/modprobe.d/tipc.conf
else
  echo -e "# Disable per security requirements" >> /etc/modprobe.d/tipc.conf
  echo "install tipc /bin/true" >> /etc/modprobe.d/tipc.conf
fi
```

NASA-ASCS-20223: Configure auditd flush priority

NASA ASCS ID	NASA-ASCS-20223
Severity	**Low**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-05
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM
Control Setting	incremental_async

The `auditd` service can be configured to synchronously write audit event data to disk. Add or correct the following line in `/etc/audit/auditd.conf` to ensure that audit event data is fully synchronized with the log files on the disk:

```
flush = incremental_async
```

Rationale

Audit data should be synchronously written to disk to ensure log integrity. These parameters assure that all audit event data is fully synchronized with the log files on the disk.

bash fix

```
AUDITCONFIG=/etc/audit/auditd.conf
AUDITCONF_ITEM="flush"
AUDITCONF_VALUE="incremental_async"

if [[ "$(grep -E "^(\s+)?$AUDITCONF_ITEM(\s+)?=(\s+)?.*$" $AUDITCONFIG)" ]]
then
  sed -i
"s/^\(\s\+\)\?$AUDITCONF_ITEM\(\s\+\)\?=\(\s\+\)\?.*$/\1$AUDITCONF_ITEM\2=\3$AUDITCONF_VALUE/"
$AUDITCONFIG
else
```

```
  echo "$AUDITCONF_ITEM = $AUDITCONF_VALUE" >> $AUDITCONFIG
fi
```

NASA-ASCS-20224: Configure auditd space_left on Low Disk Space

NASA ASCS ID	NASA-ASCS-20224
Severity	**Low**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-05
STIG Reference	RHEL_8_STIG RHEL-08-030730
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.2.3
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM
Control Setting	100

The `auditd` service can be configured to take an action when disk space is running low but prior to running out of space completely. Edit the file `/etc/audit/auditd.conf` . Add or modify the following line, substituting a positive value appropriately:

```
space_left = 100
```

Setting this value to the appropriate size in Megabytes will cause the system to notify the user of an issue.

Rationale

Notifying administrators of an impending disk space problem may allow them to take corrective action prior to any disruption.

bash fix

```
AUDITCONFIG=/etc/audit/auditd.conf
AUDITCONF_ITEM="space_left"
AUDITCONF_VALUE="100"

if [[ "$(grep -E "^(\s+)?$AUDITCONF_ITEM(\s+)?=(\s+)?.*$" $AUDITCONFIG)" ]]
then
  sed -i
"s/^\(\s\+\)\?$AUDITCONF_ITEM\(\s\+\)\?=\(\s\+\)\?.*$/\1$AUDITCONF_ITEM\2=\3$AUDITCONF_VALUE/"
$AUDITCONFIG
else
  echo "$AUDITCONF_ITEM = $AUDITCONF_VALUE" >> $AUDITCONFIG
```

```
fi
```

NASA-ASCS-20225: Configure auditd space_left Action on Low Disk Space

NASA ASCS ID	NASA-ASCS-20225
Severity	**Low**
Group	auditing/system
NIST SP 800-53r5 Reference	AU-05
STIG Reference	RHEL_8_STIG RHEL-08-030731
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 4.1.2.3
MITRE ATT&CK Reference	M1047
MITRE D3FEND Reference	D3-OSM
Control Setting	email

The `auditd` service can be configured to take an action when disk space starts to run low. Edit the file `/etc/audit/auditd.conf` . Modify the following line, substituting a value appropriately:

```
space_left_action = ACTION
```

Possible values for ACTION are described in the `auditd.conf` man page. These include:

- `syslog`
- `email`
- `exec`

Rationale

Notifying administrators of an impending disk space problem may allow them to take corrective action prior to any disruption.

bash fix

```
AUDITCONFIG=/etc/audit/auditd.conf
AUDITCONF_ITEM="space_left_action"
AUDITCONF_VALUE="email"

if [[ "$(grep -E "^(\s+)?$AUDITCONF_ITEM(\s+)?=(\s+)?.*$" $AUDITCONFIG)" ]]
then
  sed -i
"s/^\(\s\+\)\?$AUDITCONF_ITEM\(\s\+\)\?=\(\s\+\)\?.*$/\1$AUDITCONF_ITEM\2=\3$AUDITCONF_VALUE/"
```

```
$AUDITCONFIG
else
  echo "$AUDITCONF_ITEM = $AUDITCONF_VALUE" >> $AUDITCONFIG
fi
```

NASA-ASCS-20233: Verify that System Executables Have Root Ownership

NASA ASCS ID	NASA-ASCS-20233
Severity	**Low**
Group	permissions/system
NIST SP 800-53r5 Reference	AC-03 (7)
STIG Reference	RHEL_8_STIG RHEL-08-010310
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.10
MITRE ATT&CK Reference	T1222, M1022
MITRE D3FEND Reference	D3-LFP

System executables are stored in the following directories by default:

```
/bin
/sbin
/usr/bin
/usr/libexec
/usr/local/bin
/usr/local/sbin
/usr/sbin
```

All files in these directories should be owned by the `root` user. If any file in these directories found to be owned by a user other than root, correct its ownership with the following command:

```
chown root FILE
```

Rationale

System binaries are executed by privileged users as well as system services, and restrictive permissions are necessary to ensure that their execution of these programs cannot be co-opted.

bash fix

```
for BINDIR in /bin /sbin /usr/bin /usr/libexec /usr/local/bin /usr/local/sbin /usr/sbin
do
  if [ -d $BINDIR ]
```

```
  then
    find -L $BINDIR \! -user root -exec chown root {} \;
  fi
done
```

NASA-ASCS-20238: Add noexec Option to /var/tmp

NASA ASCS ID	NASA-ASCS-20238
Severity	**Low**
Group	permissions/system
STIG Reference	RHEL_8_STIG RHEL-08-040134
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.1.4.2
MITRE ATT&CK Reference	T1059, T1564, TA0002
MITRE D3FEND Reference	D3-LFP

The `noexec` mount option can be used to prevent binaries from being executed out of `/var/tmp` . Add the `noexec` option to the fourth column of `/etc/fstab` for the line which controls mounting of `/var/tmp` .

Rationale

Allowing users to execute binaries from world-writable directories such as `/var/tmp` should never be necessary in normal operation and can expose the system to potential compromise.

bash fix

```
FSTAB_FILE=/etc/fstab
if [[ "$( grep -vE "^#" $FSTAB_FILE | grep /var/tmp | grep -v noexec )" ]]
then
  sed -r -i "s/^(.*)\s+(\/var\/tmp)\s+(.*)\s+(.*)\s+(.*)\s+(.*)$/\1\t\2\t\3\t\4,noexec \5 \6/"
$FSTAB_FILE
fi
```

NASA-ASCS-20243: Uninstall tftp-server Package

NASA ASCS ID	NASA-ASCS-20243
Severity	**Low**
Group	obsolete/services
STIG Reference	RHEL_8_STIG RHEL-08-040190
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 2.2.9

MITRE ATT&CK Reference	TA0008, T1210, M1042

The `tftp-server` package can be removed with the following command:

```
yum erase tftp-server
```

or

```
apt-get remove tftp-server
```

or

```
zypper remote atftp
```

Rationale

Removing the `tftp-server` package decreases the risk of the accidental (or intentional) activation of tftp services.

If TFTP is required for operational support (such as transmission of router configurations), its use must be documented with the Information Systems Securty Manager (ISSM), restricted to only authorized personnel, and establish access control rules.

bash fix

```
if [[ "$OS_LIKE" == "fedora" ]]
then
  if rpm -q tftp-server &> /dev/null
  then
    yum -y remove tftp-server &> /dev/null
  fi
elif [[ "$OS_LIKE" == "debian" ]]
then
  if [[ "$( dpkg-query -W -f '${db:Status-Status}' tftp-server )" == "installed" ]]
  then
    apt-get -y purge tftp-server &> /dev/null
  fi
elif [[ "$OS_LIKE" == "suse" ]]
then
  if rpm -q atftp &> /dev/null
  then
    zypper --non-interactive remove atftp &> /dev/null
  fi
fi
```

NASA-ASCS-20264: Ensure No Daemons are Unconfined by SELinux

NASA ASCS ID	NASA-ASCS-20264
Severity	**Low**
Group	mandatory_access_control
NIST SP 800-53r5 Reference	AC-03 (3)
MITRE ATT&CK Reference	T1543, M1028
MITRE D3FEND Reference	D3-SCP

Daemons for which the SELinux policy does not contain rules will inherit the context of the parent process. Because daemons are launched during startup and descend from the `init` process, they inherit the `initrc_t` context. In the NASA Environment the Symantec, BigFix and AnyConnect clients are running unconfined.

To check for unconfined daemons, run the following command:

```
ps -eZ | egrep "initrc" | egrep -vw
"tr|ps|egrep|bash|awk|BESClient|XBESClientUI|vpnagentd|symcfgd|rtvscand" | tr ':' ' ' | awk '{
print $NF }'
```

It should produce no output in a well-configured system.

Rationale

Daemons which run with the `initrc_t` context may cause AVC denials, or allow privileges that the daemon does not require.

NASA-ASCS-20265: Disable Red Hat Subscription Manager Daemon (rhsmcertd)

NASA ASCS ID	NASA-ASCS-20265
Severity	**Low**
Group	base/services

The Red Hat Subscription Manager (rhsmcertd) periodically checks for changes in the entitlement certificates for a registered system and updates it accordingly. The `rhsmcertd` service can be disabled with the following command:

```
systemctl disable rhsmcertd.service
```

Rationale

The `rhsmcertd` service can provide administrators with some additional control over which of their systems are entitled to particular subscriptions. However, for systems that are managed locally or which are not expected to

require remote changes to their subscription status, it is unnecessary and can be disabled.

bash fix

```
if which systemctl &> /dev/null
then
  SERVICE=$( systemctl list-unit-files | grep -E "^(\s+)?rhsmcertd(d)?\.service" | sed "s/^\s\+//"
| cut -d" " -f1 )
  if systemctl is-active $SERVICE &> /dev/null
  then
    systemctl stop $SERVICE &> /dev/null
  fi
  if systemctl is-enabled $SERVICE &> /dev/null
  then
    systemctl disable $SERVICE &> /dev/null
  fi
else
  SERVICE=$( chkconfig | grep "^rhsmcertd" | cut -d" " -f1 )
  chkconfig $SERVICE off &> /dev/null
  service $SERVICE stop &> /dev/null
fi
```

NASA-ASCS-20291: Disable Kernel Support for USB via Bootloader Configuration

NASA ASCS ID	NASA-ASCS-20291
Severity	**Low**
Group	permissions/system

All USB support can be disabled by adding the `nousb` argument to the kernel's boot loader configuration. To do so, append "nousb" to the kernel line in `/etc/default/grub` as shown:

```
kernel /vmlinuz-VERSION ro vga=ext root=/dev/VolGroup00/LogVol00 rhgb quiet nousb
```

Additional information on kernel parameters can be found here: https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html

Additional information on grub configuration can be found here: https://www.gnu.org/software/grub/manual/grub/html_node/Simple-configuration.html#Simple-configuration

Rationale

Disabling the USB subsystem within the Linux kernel at system boot will protect against potentially malicious USB devices, although it is only practical in specialized systems.

NASA-ASCS-20293: Disable Print Server Capabilities

NASA ASCS ID	NASA-ASCS-20293
Severity	**Low**
Group	printing/services
MITRE ATT&CK Reference	M1042

To prevent remote users from potentially connecting to and using locally configured printers, disable the Common Unix Printing System (CUPS) print server sharing capabilities. To do so, limit how the server will listen for print jobs by removing the more generic port directive from /etc/cups/cupsd.conf:

```
Port 631
```

and replacing it with the `Listen` directive:

```
Listen localhost:631
```

This will prevent remote users from printing to locally configured printers while still allowing local users on the system to print normally.

Rationale

By default, locally configured printers will not be shared over the network, but if this functionality has somehow been enabled, these recommendations will disable it again. Be sure to disable outgoing printer list broadcasts, or remote users will still be able to see the locally configured printers, even if they cannot actually print to them. To limit print serving to a particular set of users, use the Policy directive.

NASA-ASCS-20356: All Interactive User Home Directories Must Be Owned By The Primary User

NASA ASCS ID	NASA-ASCS-20356
Severity	**Low**
Group	accounts/system
NIST SP 800-53r5 Reference	AC-03 (3)
STIG Reference	RHEL_8_STIG RHEL-08-010750
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 6.2.10
MITRE ATT&CK Reference	T1222, M1022
MITRE D3FEND Reference	D3-LFP

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

```
$ sudo chown USER /home/USER
```

Rationale

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

NASA-ASCS-20357: Verify that Interactive Boot is Disabled

NASA ASCS ID	NASA-ASCS-20357
Severity	**Low**
Group	accounts/system

Linux systems support an "interactive boot" option that can be used to prevent services from being started. Interactive boot can be enabled by providing a `1` , `yes` , `true` , or `on` value to the `systemd.confirm_spawn` kernel argument in `/etc/default/grub`.

Check for setting:

```
grep -E "systemd\.confirm_spawn=(1|yes|true|on)" /etc/default/grub
```

Edit the `/etc/default/grub` file to remove the systemd.config_spawn value.

update grub

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

Additional information on kernel parameters can be found here: https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html

Additional information on grub configuration can be found here: https://www.gnu.org/software/grub/manual/grub/html_node/Simple-configuration.html#Simple-configuration

Rationale

Using interactive boot, the console user could disable auditing, firewalls, or other services, weakening system security.

bash fix

```
CONFIRM_SPAWN_YES="systemd.confirm_spawn=\(1\|yes\|true\|on\)"
CONFIRM_SPAWN_NO="systemd.confirm_spawn=no"

if grep -q "\(GRUB_CMDLINE_LINUX\|GRUB_CMDLINE_LINUX_DEFAULT\)" /etc/default/grub
```

```
then
    sed -i "s/${CONFIRM_SPAWN_YES}/${CONFIRM_SPAWN_NO}/" /etc/default/grub
fi

if which rpm &> /dev/null
then
  for GRUBCFG in $( find /boot -name grub.cfg )
  do
    grub2-mkconfig -o $GRUBCFG
  done
elif which dpkg &> /dev/null
then
  update-grub
else
  echo "could not determine configuration"
fi
```

NASA-ASCS-20370: Ensure File Integrity Monitoring Software is Installed

NASA ASCS ID	NASA-ASCS-20370
Severity	**Low**
Group	software/system
STIG Reference	RHEL_8_STIG RHEL-08-010360, RHEL_8_STIG RHEL-08-010359
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 1.3.1
MITRE ATT&CK Reference	T1565
MITRE D3FEND Reference	D3-SFA

Implementations of file integrity monitor software are available in the core distributions and by external vendors. Following the instructions of proper implementation is essential to a properly configured system.

Acceptable options:

1. Aide
2. Samhien
3. Tripwire

Rationale

File integrity monitoring can expose inappropriate behavior on a system, by managing a file integrity monitor software, the System Owner can be alerted to changes to important files that could indicate a threat.

NASA-ASCS-40031: (OpenSSH) Set Address Family for IPv4 and IPv6

NASA ASCS ID	NASA-ASCS-40031
Severity	**Low**
Group	ssh/services
Control Setting	any

This setting specifies which address family is used by `sshd`.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
AddressFamily any
```

Rationale

Federal systems are required to support the transition to IPv6. Setting this value to `any` ensures that `sshd` can communicate using the current IPv4 standards as well as preparing for the future deployments based on IPv6.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^AddressFamily"
SED_INLINE="s/^AddressFamily.*$/AddressFamily any/"
ECHO_APPEND="AddressFamily any"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40034: (OpenSSH) Set Authentication Methods to publickey

NASA ASCS ID	NASA-ASCS-40034
Severity	**Low**
Group	ssh/services
Control Setting	publickey

This setting specifies the authentication methods that must be completed in order to grant access to a user.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
AuthenticationMethods    publickey
```

Rationale

Enforcing `publickey` will result in requiring the use of publickey as the only method of authentication allowed. This will prevent the ability to use passwords or other methods of authentication.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^AuthenticationMethods"
SED_INLINE="s/^AuthenticationMethods.*$/AuthenticationMethods publickey/"
ECHO_APPEND="AuthenticationMethods publickey"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40041: (OpenSSH) Disable GSSAPI Authentication

NASA ASCS ID	NASA-ASCS-40041
Severity	**Low**
Group	ssh/services
STIG Reference	RHEL_8_STIG RHEL-08-010522
MITRE ATT&CK Reference	M1042
Control Setting	no

This setting specifies whether user authentication based on Generic Security Service Application Program Interface (GSSAPI) is allowed.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
GSSAPIAuthentication no
```

For systems configured with the Centrify PIV solution, GSSAPI has been given special allowance and the these systems will not be scored as noncompliant.

Rationale

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 ***SHALL*** be disabled unless needed.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^GSSAPIAuthentication"
SED_INLINE="s/^GSSAPIAuthentication.*$/GSSAPIAuthentication no/"
ECHO_APPEND="GSSAPIAuthentication no"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
```

```
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40050: (OpenSSH) Set Type of Service and DSCP on IP Header

NASA ASCS ID	NASA-ASCS-40050
Severity	**Low**
Group	ssh/services
Control Setting	lowdelay throughput

This setting specifies the IPv4 type of service or Differentiated Services Code Point (DSCP) class for the connection.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
IPQoS  lowdelay throughput
```

Rationale

Recommended for systems that have non-standard operating system defaults. The `sshd` default is acceptable.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^IPQoS"
SED_INLINE="s/^IPQoS.*$/IPQoS lowdelay throughput/"
ECHO_APPEND="IPQoS lowdelay throughput"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
```

```
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40059: (OpenSSH) Set Max Unauthenticated Concurrent Sessions

NASA ASCS ID	NASA-ASCS-40059
Severity	**Low**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-05 (2)
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 1 - Workstation - 5.2.17
MITRE ATT&CK Reference	T1499
Control Setting	10:30:100

The value specified for this setting is defined by start:rate:full. Where *start* specifies the number of unauthenticated connections to the SSH daemon after which the SSH daemon will begin to drop the additional connections. The SSH daemon will then randomly drop the attempts with a probability of *rate*/100 until the *full* number of attempts is reached. Once the *full* number is reached, all additional connections will be dropped until authentication succeeds or the `LoginGraceTime` expires.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
MaxStartups     10:30:100
```

Rationale

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of `sshd` logins and prevent overwhelming the daemon.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^MaxStartups"
SED_INLINE="s/^MaxStartups.*$/MaxStartups 10:30:100/"
ECHO_APPEND="MaxStartups 10:30:100"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
```

```
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40066: (OpenSSH) Enable Printing of Last Log

NASA ASCS ID	NASA-ASCS-40066
Severity	**Low**
Group	ssh/services
NIST SP 800-53r5 Reference	AC-09
STIG Reference	RHEL_8_STIG RHEL-08-020350
Control Setting	yes

This setting specifies whether `sshd` prints the date and time of the last user login when a user logs in interactively.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
PrintLastLog yes
```

Rationale

Providing users feedback as to when accounts were last accessed facilitates user recognition and reporting of unauthorized account use.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^PrintLastLog"
SED_INLINE="s/^PrintLastLog.*$/PrintLastLog yes/"
ECHO_APPEND="PrintLastLog yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
```

```
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40080: (OpenSSH) Enable DNS Lookup for Client Connections

NASA ASCS ID	NASA-ASCS-40080
Severity	**Low**
Group	ssh/services
Control Setting	yes

This setting specifies whether `sshd` looks up the remote host name and checks that the resolved host name for the remote IP address maps back to the same IP address.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
UseDNS    yes
```

Rationale

Clients attempting to connect should always have a DNS entry.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^UseDNS"
SED_INLINE="s/^UseDNS.*$/UseDNS yes/"
ECHO_APPEND="UseDNS yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
```

```
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40082: (OpenSSH) Enable Use of Privilege Separation

NASA ASCS ID	NASA-ASCS-40082
Severity	**Low**
Group	ssh/services
Control Setting	sandbox

When enabled, SSH will create an unprivileged child process that has the privilege of the authenticated user.

`UsePrivilegeSeparation` has been deprecated since version 7.5. Adding the setting will cause `sshd` to generate unwanted log messages.

To configure the setting for OpenSSH in versions prior to 7.5, add or correct the following line in the `sshd_config` file on the system:

```
UsePrivilegeSeparation sandbox
```

Rationale

SSH daemon privilege separation causes the SSH process to drop root privileges when they are not needed, which decreases the impact of software vulnerabilities in the unprivileged section.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^UsePrivilegeSeparation"
SED_INLINE="s/^UsePrivilegeSeparation.*$/UsePrivilegeSeparation sandbox/"
ECHO_APPEND="UsePrivilegeSeparation sandbox"

if [[ "$( sshd -T -C user=root -C host=localhost -C addr=localhost | grep useprivilegeseparation )"
!= "" ]]
```

```
then
  INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
  if ls $INCLUDES &> /dev/null
  then
    CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
  fi
  FIXED=1
  for CONFIG_FILE in ${CONFFILES[*]}
  do
    if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
    then
      sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
      FIXED=0
    fi
  done
  if [[ "$FIXED" != "0" ]]
  then
    [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
    echo $ECHO_APPEND >> $CONFIG_FILE
  fi
fi
```

NASA-ASCS-40090: (OpenSSH) Enable SSH Server firewalld Firewall exception

NASA ASCS ID	NASA-ASCS-40090
Severity	**Low**
Group	ssh/services
CIS Reference	CIS_Red_Hat_Enterprise_Linux_8_Benchmark,Level 2 - Workstation - 5.2.13
Control Setting	22

By default, inbound connections to SSH's port are allowed. If the SSH server is being used but denied by the firewall, this exception should be added to the firewall configuration.

To configure `firewalld` to allow access, run the following command:

```
firewall-cmd --permanent --add-service=ssh
```

Rationale

If inbound SSH connections are expected, adding a firewall rule exception will allow remote access through the SSH port.

bash fix

```
if which firewall-cmd &> /dev/null
```

```
then
  firewall-cmd --permanent --add-service=ssh
  firewall-cmd --reload
else
  iptables -A INPUT -p tcp --dport 22 -j ACCEPT
  service iptables save
fi
```

NASA-ASCS-40091: (OpenSSH) Disable SSH Support for User Known Hosts

NASA ASCS ID	NASA-ASCS-40091
Severity	**Low**
Group	ssh/services
STIG Reference	RHEL_8_STIG RHEL-08-010520
MITRE ATT&CK Reference	T1078, M1042
Control Setting	yes

This setting specifies whether `sshd` ignores the user's `~/.ssh/known_hosts` during `HostbasedAuthentication` and uses only the system-wide known hosts file /etc/ssh/known_hosts.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
IgnoreUserKnownHosts yes
```

Rationale

SSH can allow a user authentication by using a cached remote system's public keys. Configuring this setting for the SSH daemon provides additional assurance that SSH will require a user-supplied authentication. This control is recommended, along with the required control to disable `HostbasedAuthentication`.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^IgnoreUserKnownHosts"
SED_INLINE="s/^IgnoreUserKnownHosts.*$/IgnoreUserKnownHosts yes/"
ECHO_APPEND="IgnoreUserKnownHosts yes"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
```

```
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40095: (OpenSSH) Use Only Strong Hostbased Accepted Key Types

NASA ASCS ID	NASA-ASCS-40095
Severity	**Low**
Group	ssh/services
NIST SP 800-53r5 Reference	SC-08 (1), IA-07, AC-17 (2)
MITRE ATT&CK Reference	M1041
MITRE D3FEND Reference	D3-MENCR
Control Setting	ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256

This setting specifies the key types that will be accepted for hostbased authentication as a comma-separated pattern list.

To configure the setting for OpenSSH, add or correct the following line in the `sshd_config` file on the system:

```
HostbasedAcceptedKeyTypes \ecdsa-sha2-nistp256-cert-v01@openssh.com,\ecdsa-sha2-nistp384-cert-v01@openssh.com,\ecdsa-sha2-nistp521-cert-v01@openssh.com,\ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-512,rsa-sha2-256
```

The FIPS 140 validated, OS-specific values are defined in the ASCS Specification for each OS.

As of OpenSSH v8.5p1, the `HostbasedAcceptedKeyTypes` keyword has been renamed to `HostbasedAcceptedAlgorithms`.

Rationale

Hostbased authentication should be disabled. However, in cases where hostbased authentication is needed, it is important to ensure that the correct Host Key Types are used for each server. Proper Host Key Types provide trust for known host keys in order to prevent man-in-the-middle attacks.

bash fix

```
CONFFILES=( /etc/ssh/sshd_config )
EXISTS_IF_REGEX="^HostbasedAcceptedKeyTypes"
SED_INLINE="s/^HostbasedAcceptedKeyTypes.*$/\ecdsa-sha2-nistp256-cert-v01@openssh.com,\ecdsa-sha2-
nistp384-cert-v01@openssh.com,\ecdsa-sha2-nistp521-cert-v01@openssh.com,\ssh-rsa-cert-
v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-
512,rsa-sha2-256/"
ECHO_APPEND="HostbasedAcceptedKeyTypes \ecdsa-sha2-nistp256-cert-v01@openssh.com,\ecdsa-sha2-
nistp384-cert-v01@openssh.com,\ecdsa-sha2-nistp521-cert-v01@openssh.com,\ssh-rsa-cert-
v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,rsa-sha2-
512,rsa-sha2-256"

INCLUDES=$( grep -E "^Include" /etc/ssh/sshd_config | sed 's/\s+/\ /g' | awk '{ print $2 }' )
if ls $INCLUDES &> /dev/null
then
  CONFFILES=( ${CONFFILES[*]} ${INCLUDES[*]} )
fi
FIXED=1
for CONFIG_FILE in ${CONFFILES[*]}
do
  if [[ $( grep -E $EXISTS_IF_REGEX $CONFIG_FILE ) ]]
  then
    sed -i.bak "$SED_INLINE" $CONFIG_FILE; rm -f "$CONFIG_FILE.bak"
    FIXED=0
  fi
done
if [[ "$FIXED" != "0" ]]
then
  [[ $(uname) == "Darwin" ]] && CONFIG_FILE=/etc/ssh/sshd_config.d/0-ASCS.conf ||
CONFIG_FILE=/etc/ssh/sshd_config
  echo $ECHO_APPEND >> $CONFIG_FILE
fi
```

NASA-ASCS-40560: (Linux Desktop) Disable Geolocation

NASA ASCS ID	NASA-ASCS-40560
Severity	**Low**
Group	software/desktop
MITRE ATT&CK Reference	T1614

Configure the desktop environment to disable the use of Geolocation service.

See [_configuration_options] for remediation guides for desktop environments and display managers.

Rationale

Using location data to track information system is unnecessary for regular operation of a desktop environment and sends system information to unknown or insecure endpoints.

NASA-ASCS-40563: (Linux Desktop) Disable Automounting of Media

NASA ASCS ID	NASA-ASCS-40563
Severity	**Low**
Group	software/desktop
MITRE ATT&CK Reference	M1028

Configure the desktop environment to disable automatic mounting of removable media devices that are inserted into the system.

See [_configuration_options] for remediation guides for desktop environments and display managers.

NASA-ASCS-40564: (Linux Desktop) Disable Keyboard Mapping for reboot or shutdown

NASA ASCS ID	NASA-ASCS-40564
Severity	**Low**
Group	software/desktop
STIG Reference	RHEL_8_STIG RHEL-08-040170
MITRE ATT&CK Reference	T1529

Configure the desktop environment to ensure any mapping of keyboard commands does not execute a reboot or shutdown of the system.

See [_configuration_options] for remediation guides for desktop environments and display managers.

Appendix A: Specific Operation Guidance

setroubleshoot

Some systems owners have found that performance issues have been found when the CDM checks have been run on a system. This performance hit can be troublesome. The CDM events in question are cause by the BigFix client being confined properly in its context, but calling upon other utilities, such as `auditctl` and `sshd`, to determine system settings. A feature in BigFix captures STDOUT and STDERR into a file denoted <ASCS ID>.detect.log, which is a context of `var_t` while the context of the calling resource is not. SELinux properly prevents the action from writing into the file, however due to SELinux auditing a record of the event, even without data, is recorded.

We have found that in the case that a system is running the `setroubleshoot` utility, that additional log entries from the audit log are posted into the system logs. This behavior of `setroubleshoot` can cause additional processing issues on some systems. `setroubleshoot` is loaded on systems that are running a graphical desktop and the AVC utility. The chain of events from the BigFix client being monitored by SELinux, an audit record being recorded, `setroubleshoot` analyzing the records via `audispd`, posting an alert to AVC, AVC posting an alert to the desktop environment, can cause a noticeable toll on resources.

Mitigation of this resource consumption currently is to either place a SELinux `donotaudit` entry into the system to quite the messages being generated, or to remove `setroubleshoot` from the system.

To quiet the auditing of SELinux on the specific BigFix controls

```
cat > bigfix_quiet.te << END_OF_FILE
module bigfix_quiet 1.0;

require {
        type iptables_t;
        type sshd_t;
        type var_t;
        type initrc_t;
        type auditctl_t;
        class file write;
}

#============= auditctl_t ==============

#!!!! WARNING: 'var_t' is a base type.
dontaudit auditctl_t var_t:file write;

#============= iptables_t ==============

#!!!! WARNING: 'var_t' is a base type.
dontaudit iptables_t var_t:file write;

#============= sshd_t ==============

#!!!! WARNING: 'var_t' is a base type.
dontaudit sshd_t var_t:file write;
END_OF_FILE

checkmodule -M -m -o bigfix_quiet.mod bigfix_quiet.te
```

```
semodule_package -o bigfix_quiet.pp -m bigfix_quiet.mod
semodule -i bigfix_quiet.pp
```

Appendix B: Graphical Target Configuration Options

This appendix contains guidance on how to configure desktop environments that are available to the distributions accepted by the Agency. These distributions are Red Hat Enterprise Linux, Amazon 2 Linux and Ubuntu Linux.

Gnome 3

Gnome 3 utilizes `dconf` to manage the Gnome3 instance. The `GDM` application is used for initial login authentication.

INFO: In order for the `dconf` utility to enforce preexisting settings that a user may have set, the use of the `lock/00-nasa` file enforces the change.

GDM specific settings

To disable Automatic Login to the system, ensure the `/etc/gdm/custom.conf` file `[daemon]` block does not set `AutomaticLoginEnable` to `true` and the `AutomaticLogin` is left blank.

/etc/gdm/custom.conf configuration:

```
[daemon]
AutomaticLoginEnable=false
AutomaticLogin=
TimedLoginEnable=false
```

dconf settings

The `dconf` settings are split into 2 sections, one for GDM and the other for the Gnome session. If files do not exist in the sections described, they can be created.

/etc/dconf/profile/gdm:

```
user-db:user
system-db:gdm
system-db:distro
```

/etc/dconf/profile/user:

```
user-db:user
system-db:local
system-db:site
system-db:distro
```

/etc/dconf/db/gdm.d/00-nasa:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='By accessing and using this information system, you acknowledge and consent to
the following:You are accessing a U.S. Government information system, which includes: (1) this
```

```
computer; (2) this computer network; (3) all computers connected to this network including end user
systems; (4) all devices and storage media attached to this network or to any computer on this
network; and (5) cloud and remote information services. This information system is provided for
U.S. Government-authorized use only. This system contains Controlled Unclassified Information
(CUI). You have no reasonable expectation of privacy regarding any communication transmitted
through or data stored on this information system. At any time, and for any lawful purpose, the
U.S. Government may monitor, intercept, search, and seize any communication or data transiting,
stored on, or traveling to or from this information system. You are NOT authorized to process
classified information on this information system. Unauthorized or improper use of this system may
result in suspension or loss of access privileges, disciplinary action, and civil and/or criminal
penalties.'
disable-user-list=true
allowed-failures=3
```

/etc/dconf/db/gdm.d/locks/00-nasa:

```
/org/gnome/login-screen/banner-message-enable
/org/gnome/login-screen/banner-message-text
/org/gnome/login-screen/disable-user-list
/org/gnome/login-screen/allowed-failures
```

/etc/dconf/db/local.d/00-nasa:

```
[org/gnome/desktop/screensaver]
lock-enabled=true
lock-delay=uint32 1

[org/gnome/desktop/session]
idle-delay=uint32 600

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

The use of the `logout=''` is important, some versions of `dconf` require the `''` while others do not. Since we only want to make a single check the compliance will be looking for the `''` as a result.

/etc/dconf/db/local.d/locks/00-nasa:

```
/org/gnome/desktop/screensaver/lock-enabled
/org/gnome/desktop/screensaver/lock-delay
/org/gnome/desktop/session/idle-delay
/org/gnome/settings-daemon/plugins/media-keys/logout
```

Once completed, updates to the dconf files update the database with the following command:

```
dconf update
```

Dconf optional settings

Location Service Disabling

/etc/dconf/db/local.d/00-nasa

```
[org/gnome/system/location]
enabled=false
```

/etc/dconf/db/local.d/locks/00-nasa:

```
/org/gnome/system/location/enabled
```

Media Automount Disabling

/etc/dconf/db/local.d/00-nasa

```
[org/gnome/desktop/media-handling]
automount=false
automount-open=false
autorun-never=true
```

/etc/dconf/db/local.d/locks/00-nasa

```
/org/gnome/desktop/media-handling/automount
/org/gnome/desktop/media-handling/automount-open
/org/gnome/desktop/media-handling/autorun-never
```

SDDM and KDE 5

Controls have not been fully determined to sufficiently assess whether KDE 5 and SDDM are fully compliant. The work to determine these controls is ongoing. If the community is able to determine the best method for implementation of SDDM and KDE 5 to meet the required controls, please provide ASCS with the method of implementing the cotrols, so ASCS can determine how they can be assessed.

SDDM

/etc/sddm.conf

```
[User]
MinimumUid=60000
MaximumUid=60000
HideUsers=true
RememberLastUser=false
RememberLastSession=false

[AutoLogin]
Session=
```

```
User=
Relogin=
```

KDE 5

While it is accepted by KDE to place the screenlock actions into multiple different files, we ask that - if using KDE 5 - to place the commands into `/etc/xdg/kscreenlockerrc`. This will provide a consistent location in the file system to provide a CDM check that does not place extra strain on a system by doing a massive file search to find all the available KDE locations and setting files.

/etc/xdg/kscreenlockerrc

```
[Daemon][$i]
Autolock=true
Timeout=1
```

Known Issues with SDDM and KDE 5

Controls have not been fully determined to sufficiently assess whether KDE 5 and SDDM are fully compliant. The work to determine these controls is ongoing. If the community is able to determine the best method for implementation of SDDM and KDE 5 to meet the required controls, please provide ASCS with the method of implementing the controls, so a method can be created to determine how they can be assessed.

KDE 5 has the capacity to set the `Ctrl-Alt-Del` keyboard mapping for a user session through graphical tools. Unfortunately it has yet to be determined how to provide an acceptable solution to override the mapping from the system level.

Gnome 2

GDM

The elements for the GDM configuration can follow the same for the Gnome 3 GDM section.

Configuration gconf

The following entries will need to be updated in the `/etc/gconf/gconf.xml.defaults/%gconf-tree.xml` file. In most situations, the entries can be searched for, and the default value can be replaced.

As of specification version v1.0.1 the change and the fix now uses the gconftool-2.

Disable User List

```
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type bool --set /apps/gdm/simple-greeter/disable_user_list true
```

Prevent ctrl-alt-del from prompting for reboot

```
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type string --set /apps/gnome_settings_daemon/keybindings/power ""
```

Enable banner message

```
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type bool --set /apps/gdm/simple-greeter/banner_message_enable true
```

Set banner text

```
# NOTE: Direct copy and paste may not work from document
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type string --set /apps/gdm/simple-greeter/banner_message_text "By accessing\
 and using this information system, you acknowledge and consent to the following:\
 You are accessing a U.S. Government information system, which includes: (1) this\
 computer; (2) this computer network; (3) all computers connected to this network\
 including end user systems; (4) all devices and storage media attached to this\
 network or to any computer on this network; and (5) cloud and remote information\
 services. This information system is provided for U.S. Government authorized use\
 only. You have no reasonable expectation of privacy regarding any communication\
 transmitted through or data stored on this information system. At any time, and\
 for any lawful purpose, the U.S. Government may monitor, intercept, search, and\
 seize any communication or data transiting, stored on, or traveling to or from\
 this information system. You are NOT authorized to process classified information\
 on this information system. Unauthorized or improper use of this system may result\
 in suspension or loss of access privileges, disciplinary action, and civil and/or\
 criminal penalties."
```

Enable screen locking

```
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type bool --set /apps/gnome-screensaver/lock_enabled true
```

Set lock delay

```
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type int --set /apps/gnome-screensaver/lock_delay 0
```

Set idle delay

```
gconftool-2 --direct --config-source=xml:readwrite:/etc/gconf/gconf.xml.defaults \
  --type int --set /apps/gnome-screensaver/idle_delay 15
```

For the number of retries setting, set at the top of the `gdm-password` PAM config file, prior to the line with `password-auth` inclusion:

/etc/pam.d/gdm-password

```
auth       required     pam_tally2.so deny=3 even_deny_root lock_time=60 unlock_time=3000
```

Unity and lightDM

Configuration for lightDM

The `lightdm.conf` file shown here is arbitrary, use of users.conf, or lightdm.conf.d/lightdm.conf is also acceptable.

/etc/lightdm/lightdm.conf

```
[SeatDefaults]
autologin-user=
autologin-user-timeout=
greeter-hide-users=true
greeter-show-manual-login=true
allow-guest=false
session-setup-script=xmessage -f /etc/issue
```

Configuration for dconf

Unity uses dconf for some of its settings. To configure dconf in the Unity environment, follow the changes for the `/etc/dconf/db/local.d` and `/etc/dconf/profile/user` in Gnome 3.

KDM and KDE4

Controls have not been fully determined to sufficiently assess whether KDE 4 and KDM are fully compliant. The work to determine these controls is ongoing. If the community is able to determine the best method for implementation of KDM and KDE 4 to meet the required controls, please provide ASCS with the method of implementing the controls, so a method can be created to determine how they can be assessed.

RHEL 6 KDE4 instance uses the GDM login application, configuration for the Gnome2 GDM components should be initiated and the following KDE session changes should be added.

KDM

The `kdmrc` file can make sure the auto login features are overridden.

/etc/kde/kdm/kdmrc

```
[X-*-Core]
AutoLoginEnable=false
```

KDE 4

The screen locking settings should be placed into the `kdeglobals` configuration file. Note that the `[$i]` component is

optional and that it flags the block to prevent users from changing the setting.

/usr/share/kde-settings/kde-profiles/default/share/config/kdeglobals

```
[ScreenSaver][$i]
Enabled=true
LegacySaverEnabled=false
Lock=true
LockGrace=1000
Timeout=900
```

Known Issues with KDM and KDE 4

ASCS does not currently have a way to provide a means of enforcing a issue banner and the compliance check in the KDM or KDE 4 desktop environment. KDM does have theming options that can provide an image of the banner and other alternative approaches, but these are currently not able to be consistently checked for compliance.

KDE 4 has the capacity to set the `Ctrl-Alt-Del` keyboard mapping for a user session through graphical tools. Unfortunately it has yet to be determined how to provide an acceptable solution to override the mapping from the system level.

Appendix C: General Initial Setup Guidance

In order to better utilize this specification, this section will provide general operational guidance that an ISO can use to bring a system to full configuration compliance. There are three phases of implementation of a new system that will be covered: installation, first boot, and continued operation.

Installation

During the base OS installation process, in order to comply with some elements of the specification, the following elements shall be configured:

- Disk Partitioning - **Required at installation**.
- LUKS: Data at Rest (DAR) - **Required at installation**.
- Network Configuration - Recommended at installation, can be completed later.
- First User - Recommended during installation, can be removed later.

These settings can be implemented manually using the installer application, or can be configured using a kickstart file.

Disk Partitioning

The [_specification] contains details of all the controls that must be configured on a compliant system. The following disk partitions shall be created:

- `/tmp` - [_ensure_tmp_located_on_separate_partition]
- `/var/tmp` - [_ensure_vartmp_located_on_separate_partition]
- `/var/log` - [_ensure_varlog_located_on_separate_partition]
- `/var/log/audit` - [_ensure_varlogaudit_located_on_separate_partition]

The partition utility in the graphical installer also shall have a `/boot`, `/` (directory root), and a swap partition.

An example of a kickstart file partition entry:

```
clearpart --all --initlabel

part /boot --fstype="ext4" --size=512
part swap --size=2048
part pv.01 --grow

volgroup rhel pv.01

logvol /tmp --fstype="ext4" --size=1024 --vgname=rhel --name=lv_tmp
logvol /var/log --fstype="ext4" --size=1024 --vgname=rhel --name=lv_var_log
logvol /var/log/audit --fstype="ext4" --size=1024 --vgname=rhel --name=lv_var_log_audit
logvol /var/tmp --fstype="ext4" --size=1024 --vgname=rhel --name=lv_var_tmp
logvol / --fstype="ext4" --grow --size=1 --vgname=rhel --name=lv_root
```

LUKS: Data at Rest (DAR)

The Agency Security Configuration Standards (ASCS) page contains the NASA-HDBK-2602 *Data At Rest Handbook*.

Network Configuration

The installation saves time by updating the network settings (`/etc/sysconfig/network-scripts` files) and host name settings (`/etc/hostname`)

Example of kickstart settings for network:

```
network  --bootproto=dhcp --device=enp1s0f0 --onboot=on --ipv6=auto --activate \
         --hostname=<hostname.of.the.system>
```

First User

Creating a new user on the system will allow access without utilizing the root account: (See: [_disallow_direct_root_logins], [_restrict_virtual_console_root_logins], [_restrict_serial_port_root_logins], [_disable_ssh_root_login])

The account can later be disabled if the system is utilizing domain accounts (such as integrated with Active Directory or the Red Hat idM product).

Example of a kickstart entry for setting a root password and a user account:

```
rootpw --iscrypted ...<hashed text string>...
user --gid=1000 --uid=1000 --name=breakglass --gecos="Break Glass Account" --groups=wheel \
     --password=...<hashed text string>... --iscrypted
```

First Boot

Initial tasks to access the software packages and implement the security configurations can be performed manually, or they can be configured during the kickstart process (using %post blocks).

Registering the System

Access to Red Hat Satellite product or directly to Red Hat Access requires valid licensing of Red Hat products to complete a proper registration of the system.

Bash command:

```
sudo subscription-manager register
```

Example of kickstart command:

```
%post
logger "Starting anaconda postinstall"
exec < /dev/tty3 > /dev/tty3
#changing to VT 3 so that we can see whats going on....
/usr/bin/chvt 3
```

```
(
# add subscription manager
yum -t -y -e 0 install subscription-manager
subscription-manager register --activationkey=<predefined activation key>
%end
```

Updating All of the Packages

Once the system is registered, update all packages.

Update the current packages:

```
sudo yum update -y
# reboot may be required if kernel has been updated
#sudo reboot
```

The `yum update -y` command can be added to the above kickstart file block to run it during the `%post` block.

Install Needed Packages

This step can also be done during the Updating All of the Packages step and can likewise be added to the kickstart `%packages` block. The `scap-security-guide` package, and its dependencies, will provide the tools needed for automated system remediation. The remediation automation is provided by the `scap-security-guide` developers, thus not maintained or authored by ASCS. If uncomfortable with the use of such a tool, this specification contains Bash Shell fix text to show how to update the settings manually.

Getting the `scap-security-guide`:

```
sudo yum install scap-security-guide -y
```

An Example of the kickstart block:

```
%packages --ignoremissing
@^minimal
@core
openscap
openscap-scanner
scap-security-guide
%end
```

Continued Operation

During operation of the system, it is the responsibility of the ISO to maintain compliance to the current specification. Updates to the specification may occur during a vendor point release, if security vulnerabilities are found, or if deficiencies are identified in the specification. The ASCS Website provides a news feed on specification changes. To subscribe to the nasa-ascs-technical mailing list for update announcements go to ASCS technical mailing list information.

Package Updates

Security patches and fixes are a regular occurrence, and ISOs are expected to maintain current security patches on systems. The system security plan (SSP) will have controls detailing the expected time to implement updates.

Maintaining a Clean Package Database

During continued operations and updates to the system, the package database may begin deviating from the actual files on the system. It is a good practice to implement regular checking and clean up of the package database. The OpenSCAP check for `rpm_verify_hash` and `rpm_verify_permissions` provide the ability to score the health of the package database and the associated files. However, these checks conflict with other, more important, configuration setting checks in the specification.

The value added by monitoring the health of the package database should be determined by the ISO and documented in the SSP, and the management and remediation of issues with it are the responsibility of the ISO.

Checking the package database health:

```
rpm -Va --nodeps --noghost --noscripts --noconfig --nolinkto
```

This will display issues that should be investigated and resolved.

In some cases the duplicate packages are on a system from a previous upgrade and can be cleaned automatically. The automation requires the `yum-utils` package.

Cleaning up duplicates in the package database:

```
package-cleanup --removedupes
```

In some cases manual cleanup of packages will be necessary.

It is a good practice to also monitor files on the system that are not associated to an RPM for the set-user-id (SUID) or the set-group-id (SGID) permission flag. The OpenSCAP checks for `file_permissions_unauthorized_sgid` and `file_permissions_unauthorized_suid` provide the ability to score files that are set to allow SGID or SUID action, but any time a system has a complied driver or is running in a virtual environment, the checks will result in failure.

Like the package database health, the ISO should regularly monitor the system allowance of SUID and SGID permissions on files.

Finding Files with SUID Not in The Package Database:

```
#!/bin/bash
# Exclude due to noexec compliance or managed in userspace
EX_DIRS=(/dev /proc /tmp /var/tmp /run/user /run/media)
EXCLUDE=
for d in ${EX_DIRS[*]}
do
  EXCLUDE=$EXCLUDE"-path $d -o "
done

# Only 1 TO_CHECK should be uncommented.
# Checking SUID
TO_CHECK=( $( find / \( ${EXCLUDE:0: -3} \) -prune -o -type f -perm /4000 ) )
```

```
# Checking SGID
#TO_CHECK=( $( find / \( ${EXCLUDE:0: -3} \) -prune -o -type f -perm /2000 ) )

for chk in ${TO_CHECK[*]}
do
  # exclude if its one of the prune directories (currently ends up in output)
  if [[ ! "$( stat -c %F $chk )" == "directory" ]]
  then
    # see if file is packaged is from rpm database
    PKG="$( rpm -q --whatprovides $chk )"
    if [[ "$PKG" == *"is not owned by any package" ]]
    then
      echo "$chk is not owned by signed package in rpm database, needs manually fixed."
    else
      # verify the rpm associated to file found with suid flag.
      # we only concerns are with files that rpms are not signed
      PKG_CHK="$(rpm -V $PKG --nodeps --nodigest --noconfig --nofiles --noghost --noscripts
--nolinkto --nofiledigest --nosize --nouser --nogroup --nomtime --nomode --nordev )"
      if [[ ! "$PKG_CHK" == "" ]]
      then
        echo "$chk: $PKG_CHK, needs manually fixed"
      fi
    fi
  fi
done
```