CMMC Vulnerabilities

Wednesday, November 29, 2023 1:59 PM

11/29/23
OEL 8
SRG-OS-000033-GPOS-00014
OL 8 must implement NIST FIPS-validated cryptography for the following: To provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
From <http://tst-tstla-201.oracle.eagle.org/STIG/tst-tstla-201-eval.html>
Remediation
Configure the operating system to implement DOD-approved encryption by following the steps below: To enable strict FIPS compliance, the fips=1 kernel option must be added to the kernel boot parameters during system installation so key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Enable FIPS mode after installation (not strict FIPS-compliant) with the following command: $ sudo fips-mode-setup --enable Reboot the system for the changes to take effect.
From <http://tst-tstla-201.oracle.eagle.org/STIG/tst-tstla-201-eval.html>
(Fips require to be fully implemented during server build config)
fips-mode-setup --enable (This changes only apply for testing purposes and does not apply full generation)
reboot

SRG-OS-000073-GPOS-00041
The OL 8 shadow password suite must be configured to use a sufficient number of hashing rounds.
Remediation
Configure OL 8 to encrypt all stored passwords with a strong cryptographic hash. Edit/modify the following line in the "/etc/login.defs" file and set "SHA_CRYPT_MIN_ROUNDS" to a value no lower than "5000": SHA_CRYPT_MIN_ROUNDS 5000
vi /etc/login.defs
add the line.. SHA_CRYPT_MIN_ROUNDS 5000

SRG-OS-000080-GPOS-00048
OL 8 operating systems booted with a BIOS must require authentication upon booting into single-user and maintenance modes.
Remediation:
Configure the system to require a grub bootloader password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the "/boot/grub2/user.cfg" file. Generate an encrypted grub2 password for the grub superusers account with the following command: $ sudo grub2-setpassword Enter password: Confirm password:
grub2-setpassword
reboot

SRG-OS-000126-GPOS-00066
OL 8 must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.
Remediation:
Note: This setting must be applied in conjunction with OL08-00-010201 to function correctly. Configure the SSH server to terminate a user session automatically after the SSH client has become unresponsive. Modify or append the following line in the "/etc/ssh/sshd_config" file: ClientAliveCountMax 1 For the changes to take effect, the SSH daemon must be restarted. $ sudo systemctl restart sshd.service
vi /etc/ssh/sshd_config
modify the line: ClientAliveCountMax 1
systemctl restart sshd.service

SRG-OS-000480-GPOS-00232 1x fail
The OL 8 SSH server must be configured to use strong entropy.
Remediation:
Configure the operating system SSH server to use strong entropy. Add or modify the following line in the "/etc/sysconfig/sshd" file. SSH_USE_STRONG_RNG=32 The SSH service must be restarted for changes to take effect.
vi /etc/sysconfig/sshd
modify and set: SSH_USE_STRONG_RNG=32
systemctl restart sshd.service

SRG-OS-000366-GPOS-00153
OL 8 must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.
Remediation:
Configure the operating system to remove all software components after updated versions have been installed. Set the "localpkg_gpgcheck" option to "True" in the "/etc/dnf/dnf.conf" file: localpkg_gpgcheck=True
vi /etc/dnf/dnf.conf
add the line: localpkg_gpgcheck=True

###After updating and installing software components, you can use the dnf package manager to remove the old versions of the software. For example, to remove all old versions of installed packages:
sudo dnf autoremove …

SRG-OS-000138-GPOS-00069
OL 8 must restrict access to the kernel message buffer.
Remediation:
Configure OL 8 to restrict access to the kernel message buffer. Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory: kernel.dmesg_restrict = 1 Remove any configurations that conflict with the above from the following locations: /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf /etc/sysctl.d/*.conf Load settings from all system configuration files with the following command: $ sudo sysctl --system
vi 99-sysctl.conf
add the line: kernel.dmesg_restrict = 1
sysctl --system

SRG-OS-000138-GPOS-00069
OL 8 must prevent kernel profiling by unprivileged users.
Remediation:
Configure OL 8 to prevent kernel profiling by unprivileged users. Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory: kernel.perf_event_paranoid = 2 Remove any configurations that conflict with the above from the following locations: /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf /etc/sysctl.d/*.conf Load settings from all system configuration files with the following command: $ sudo sysctl --system
vi 99-sysctl.conf
add the line: kernel.perf_event_paranoid = 2

sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must use the invoking user's password for privilege escalation when using "sudo".
Remediation description:
Define the following in the Defaults section of the /etc/sudoers file or a configuration file in the /etc/sudoers.d/ directory: Defaults !targetpw Defaults !rootpw Defaults !runaspw Remove any configurations that conflict with the above from the following locations: /etc/sudoers /etc/sudoers.d/
vi /etc/sudoers.d/scap_config
add the following line: Defaults !targetpw Defaults !rootpw Defaults !runaspw

SRG-OS-000373-GPOS-00156
OL 8 must require re-authentication when using the "sudo" command.
Remediation :
Configure the "sudo" command to require re-authentication. Edit the /etc/sudoers file: $ sudo visudo Add or modify the following line: Defaults timestamp_timeout=[value] Note: The "[value]" must be a number that is greater than or equal to "0". Remove any duplicate or conflicting lines from /etc/sudoers and /etc/sudoers.d/ files.
vi /etc/sudoers.d/scap_config
add the following line: Defaults timestamp_timeout=0

SRG-OS-000480-GPOS-00227
The OL 8 SSH daemon must perform strict mode checking of home directory configuration files.
Remediation description:
Configure SSH to perform strict mode checking of home directory configuration files. Uncomment the "StrictModes" keyword in "/etc/ssh/sshd_config" and set the value to "yes": StrictModes yes The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command: $ sudo systemctl restart sshd.service
vi /etc/ssh/sshd_config
set the value: StrictModes yes
systemctl restart sshd.service

SRG-OS-000480-GPOS-00227
The OL 8 SSH daemon must not allow authentication using known host's authentication.
Remediation:
Configure the SSH daemon to not allow authentication using known host’s authentication. Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes": IgnoreUserKnownHosts yes The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command: $ sudo systemctl restart sshd.service
vi /etc/ssh/sshd_config
set the value: IgnoreUserKnownHosts yes
systemctl restart sshd.service

SRG-OS-000480-GPOS-00227
The OL 8 SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.
Remediation:
Configure the SSH daemon to not allow Kerberos authentication. Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no": KerberosAuthentication no The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command: $ sudo systemctl restart sshd.service
vi /etc/ssh/sshd_config
set the value: KerberosAuthentication no
systemctl restart sshd.service

SRG-OS-000480-GPOS-00227
The OL 8 SSH daemon must not allow GSSAPI authentication, except to fulfill documented and validated mission requirements.
Remediation:
Configure the SSH daemon to not allow GSSAPI authentication. Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no": GSSAPIAuthentication no The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command: $ sudo systemctl restart sshd.service
vi /etc/ssh/sshd_config
set the value: GSSAPIAuthentication no
systemctl restart sshd.service

SRG-OS-000480-GPOS-00229
OL 8 must not allow users to override SSH environment variables.
Remediation description:
Configure OL 8 to allow the SSH daemon to not allow unattended or automatic login to the system. Add or edit the following line in the "/etc/ssh/sshd_config" file: PermitUserEnvironment no The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command: $ sudo systemctl restart sshd.service
vi /etc/ssh/sshd_config
set the value: PermitUserEnvironment no
systemctl restart sshd.service

SRG-OS-000480-GPOS-00227
OL 8 must disable storing core dumps.
Remediation:
Configure OL 8 to disable storing core dumps for all users. Add or modify the following line in "/etc/systemd/coredump.conf": Storage=none
vi /etc/systemd/coredump.conf
set to: Storage=none

SRG-OS-000480-GPOS-00227 1x fail
OL 8 must disable core dump backtraces.
Remediation:
Configure OL 8 to disable core dump backtraces. Add or modify the following line in "/etc/systemd/coredump.conf": ProcessSizeMax=0

SRG-OS-000021-GPOS-00005
OL 8 systems, versions 8.2 and above, must automatically lock an account when three unsuccessful logon attempts occur.
Remediation :
Configure OL 8 to lock an account when three unsuccessful logon attempts occur. Add/modify the "/etc/security/faillock.conf" file to match the following line: deny = 3
vi /etc/security/faillock.conf
Add/modify: deny = 3

SRG-OS-000021-GPOS-00005
OL 8 systems, versions 8.2 and above, must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.
Remediation:
Configure OL 8 to lock an account when three unsuccessful logon attempts occur. Add/modify the "/etc/security/faillock.conf" file to match the following line: fail_interval = 900

vi /etc/security/faillock.conf
Add/modify: fail_interval = 900

SRG-OS-000021-GPOS-00005
OL 8 systems, versions 8.2 and above, must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.
Remediation:
Configure OL 8 to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes. Add/modify the "/etc/security/faillock.conf" file to match the following line: unlock_time = 0
vi etc/security/faillock.conf
Add/modify: unlock_time = 0

SRG-OS-000021-GPOS-00005
OL 8 systems, versions 8.2 and above, must prevent system messages from being presented when three unsuccessful logon attempts occur.
Remediation:
Configure the operating system to prevent informative messages from being presented at logon attempts. Add/modify the "/etc/security/faillock.conf" file to match the following line: silent
vi etc/security/faillock.conf
Uncomment: silent

SRG-OS-000021-GPOS-00005
OL 8 systems, versions 8.2 and above, must log user name information when unsuccessful logon attempts occur.
Remediation description:
Configure the operating system to log user name information when unsuccessful logon attempts occur. Add/modify the "/etc/security/faillock.conf" file to match the following line: audit
vi etc/security/faillock.conf
Uncomment: audit

SRG-OS-000021-GPOS-00005
OL 8 systems, versions 8.2 and above, must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.
Remediation:
Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes. Add/modify the "/etc/security/faillock.conf" file to match the following line: even_deny_root
vi etc/security/faillock.conf
Uncomment: even_deny_root

SRG-OS-000027-GPOS-00008 1x fail
OL 8 must limit the number of concurrent sessions to 10 for all accounts and/or account types.
Remediation:
Configure OL 8 to limit the number of concurrent sessions to 10 for all accounts and/or account types. Add the following line to the top of "/etc/security/limits.conf" or in a ".conf" file defined in "/etc/security/limits.d/": * hard maxlogins 10
HOLD

SRG-OS-000028-GPOS-00009
OL 8 must enable a user session lock until that user re-establishes access using established identification and authentication procedures for command line sessions.
Remediation:
Configure the operating system to enable a user to manually initiate a session lock via tmux. This configuration binds the uppercase letter "X" to manually initiate a session lock after the prefix key "Ctrl + b" has been sent. The complete key sequence is thus "Ctrl + b" then "Shift + x" to lock tmux. Create a global configuration file "/etc/tmux.conf" and add the following lines: set -g lock-command vlock bind X lock-session Reload tmux configuration to take effect. This can be performed in tmux while it is running: $ tmux source-file /etc/tmux.conf
HOLD

SRG-OS-000028-GPOS-00009
OL 8 must ensure session control is automatically started at shell initialization.
Remediation:
Configure the operating system to initialize the tmux terminal multiplexer as each shell is called by adding the following lines to a custom.sh shell script in the /etc/profile.d/ directory: if ["$PS1"]; then parent=$(ps -o ppid= -p $$) name=$(ps -o comm= -p $parent) case "$name" in (sshd|login) tmux ;; esac fi This setting will take effect at next logon.
HOLD

SRG-OS-000028-GPOS-00009
OL 8 must have the tmux package installed.
Remediation description:
Configure the operating system to enable a user to initiate a session lock via tmux. Install the "tmux" package, if it is not already installed, by running the following command: $ sudo yum install tmux
#dnf install tmux

SRG-OS-000028-GPOS-00009
OL 8 must prevent users from disabling session control mechanisms.
Remediation:
Configure the operating system to prevent users from disabling the tmux terminal multiplexer by editing the "/etc/shells" configuration file to remove any instances of tmux.

SRG-OS-000069-GPOS-00037 ####
OL 8 must enforce password complexity by requiring that at least one uppercase character be used.
Remediation:
Configure OL 8 to enforce password complexity by requiring that at least one uppercase character be used by setting the "ucredit" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: ucredit = -1 Remove any configurations that conflict with the above value.
vi /etc/security/pwquality.conf
Add/modify: ucredit = -1

SRG-OS-000070-GPOS-00038
OL 8 must enforce password complexity by requiring that at least one lowercase character be used.
Remediation:
Configure OL 8 to enforce password complexity by requiring that at least one lowercase character be used by setting the "lcredit" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: lcredit = -1 Remove any configurations that conflict with the above value.
vi /etc/security/pwquality.conf
Add/modify: lcredit = -1

SRG-OS-000071-GPOS-00039
OL 8 must enforce password complexity by requiring that at least one numeric character be used.
Remediation:
Configure OL 8 to enforce password complexity by requiring that at least one numeric character be used by setting the "dcredit" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: dcredit = -1 Remove any configurations that conflict with the above value.
vi /etc/security/pwquality.conf
Add/modify: dcredit = -1

SRG-OS-000072-GPOS-00040
OL 8 must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.
Remediation:
Configure OL 8 to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: maxclassrepeat = 4 Remove any configurations that conflict with the above value.
vi /etc/security/pwquality.conf
Add/modify: maxclassrepeat = 4

SRG-OS-000072-GPOS-00040
OL 8 must require the maximum number of repeating characters be limited to three when passwords are changed.
Remediation:
Configure OL 8 to require the change of the number of repeating consecutive characters when passwords are changed by setting the "maxrepeat" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: maxrepeat = 3 Remove any configurations that conflict with the above value.
vi /etc/security/pwquality.conf
Add/modify: maxrepeat = 3

SRG-OS-000072-GPOS-00040
OL 8 must require the change of at least 8 characters when passwords are changed.
Remediation:
Configure OL 8 to require the change of at least eight of the total number of characters when passwords are changed by setting the "difok" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: difok = 8 Remove any configurations that conflict with the above value.
vi /etc/security/pwquality.conf
Add/modify: difok = 8

Configure the "/etc/fstab" to use the "noexec,nodev,nosuid" option on file systems that are being imported via NFS.
(Notes need to be added)
umount /ABS/
vi /etc/fstab
noexec,nodev,nosuid
mount /ABS/

SRG-OS-000480-GPOS-00227
OL 8 must not have the "gssproxy" package installed if not required for operational support.
Nfs – utils use the package gssproxy so skip it

SRG-OS-000480-GPOS-00227
OL 8 must not have the "tuned" package installed if not required for operational support.
Yum remove tuned -y

SRG-OS-000480-GPOS-00227
OL 8 must not have the "iprutils" package installed if not required for operational support.
Yum remove iprutils

SRG-OS-000480-GPOS-00227
The OL 8 SSH daemon must prevent remote hosts from connecting to the proxy display.
vi /etc/ssh/sshd_config
from
#X11UseLocalhost yes
To
X11UseLocalhost yes
Restart sshd service
systemctl restart sshd

SRG-OS-000480-GPOS-00227
OL 8 remote X connections for interactive users must be disabled unless to fulfill documented and validated mission requirements.
vi /etc/ssh/sshd_config
from
X11Forwarding yes
To
X11Forwarding no
Restart sshd service
systemctl restart sshd

SRG-OS-000480-GPOS-00227
OL 8 must enable hardening for the Berkeley Packet Filter Just-in-time compiler.
cd /etc/sysctl.d
Vi 99-sysctl.conf
Add the following line
net.core.bpf_jit_harden = 2
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must disable the use of user namespaces.
cd /etc/sysctl.d
Vi 99-sysctl.conf
Add the following line
user.max_user_namespaces = 0
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must restrict the use of "ptrace" to descendant processes.
Cd /usr/lib/sysctl.d
Vi 10-default-yama-scope.conf
Add the following line
kernel.yama.ptrace_scope = 1
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.
sudo sysctl -w net.ipv6.conf.all.accept_redirects=0
or
cd /etc/sysctl.d
Vi 99-sysctl.conf
Add the following line
net.ipv6.conf.all.accept_redirects = 0
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.
cd /etc/sysctl.d
Vi 99-sysctl.conf
Add the following line
net.ipv4.conf.all.accept_redirects = 0
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must not allow interfaces to perform Internet Control Message Protocol (ICMP) redirects by default.
cd /etc/sysctl.d
Vi 99-sysctl.conf
Add the following line
net.ipv4.conf.default.send_redirects = 0
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must not accept router advertisements on all IPv6 interfaces by default.
cd /etc/sysctl.d
Vi 99-sysctl.conf
Add the following line
net.ipv6.conf.default.accept_ra = 0
Apply the settings
sysctl --system

SRG-OS-000480-GPOS-00227
OL 8 must not accept router advertisements on all IPv6 interfaces.(Above config same process)
net.ipv6.conf.all.accept_ra = 0

SRG-OS-000480-GPOS-00227
OL 8 must not enable IPv6 packet forwarding unless the system is a router.
net.ipv6.conf.all.forwarding = 0

SRG-OS-000480-GPOS-00227
OL 8 must not forward IPv6 source-routed packets by default.
net.ipv6.conf.default.accept_source_route = 0

SRG-OS-000480-GPOS-00227
OL 8 must not forward IPv6 source-routed packets.
net.ipv6.conf.all.accept_source_route = 0

SRG-OS-000480-GPOS-00227
OL 8 must not respond to Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.
net.ipv4.icmp_echo_ignore_broadcasts = 1

SRG-OS-000480-GPOS-00227
OL 8 must not send Internet Control Message Protocol (ICMP) redirects.
net.ipv4.conf.all.send_redirects = 0

SRG-OS-000480-GPOS-00227
OL 8 must prevent IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.
net.ipv6.conf.default.accept_redirects = 0

SRG-OS-000480-GPOS-00227
OL 8 must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.
net.ipv4.conf.default.accept_redirects = 0

SRG-OS-000480-GPOS-00227
OL 8 must not forward IPv4 source-routed packets by default.
net.ipv4.conf.default.accept_source_route = 0

.....

SRG-OS-000480-GPOS-00227
OL 8 must disable the systemd Ctrl-Alt-Delete burst key sequence.
Vi /etc/systemd/system.conf
Update
CtrlAltDelBurstAction=none

systemctl daemon-reload

SRG-OS-000033-GPOS-00014
OL 8 must force a frequent session key renegotiation for SSH connections to the server.
Vi /etc/ssh/sshd_config
Add the entry
RekeyLimit 1G 1h

systemctl restart sshd

SRG-OS-000378-GPOS-00163

OL 8 must have the USBGuard installed.
yum install usbguard.x86_64

SRG-OS-000368-GPOS-00154
The OL 8 "fapolicy" module must be installed.
yum install fapolicyd.x86_64

SRG-OS-000368-GPOS-00154
OL 8 must mount "/dev/shm" with the "noexec" option.
Add the following line to /etc/fstab
tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0

SRG-OS-000114-GPOS-00059
OL 8 must be configured to disable the ability to use USB mass storage devices.
[root@tst-tstla-91 ~]# cd /etc/modprobe.d/
[root@tst-tstla-91 modprobe.d]# vi bluetooth.conf
install usb-storage /bin/true
[root@tst-tstla-91 modprobe.d]# vi blacklist.conf
blacklist usb-storage

Reboot

SRG-OS-000300-GPOS-00118
[root@tst-tstla-91 ~]# cd /etc/modprobe.d/
[root@tst-tstla-91 modprobe.d]# vi bluetooth.conf
install bluetooth /bin/true
[root@tst-tstla-91 modprobe.d]# vi blacklist.conf
blacklist bluetooth

SRG-OS-000095-GPOS-00049
OL 8 must disable IEEE 1394 (FireWire) Support.
[root@tst-tstla-91 modprobe.d]# vi firewire-core.conf
install firewire-core /bin/true
[[root@tst-tstla-91 modprobe.d]# vi blacklist.conf
blacklist firewire-core

SRG-OS-000095-GPOS-00049
OL 8 must disable mounting of cramfs.
[root@tst-tstla-91 modprobe.d]# vi cramfs.conf
install cramfs /bin/true
[root@tst-tstla-91 modprobe.d]# vi blacklist.conf
blacklist cramfs

SRG-OS-000095-GPOS-00049
OL 8 must disable the transparent inter-process communication (TIPC) protocol.
[root@tst-tstla-91 modprobe.d]# cat tipc.conf
install tipc /bin/true
[root@tst-tstla-91 modprobe.d]# cat blacklist.conf
blacklist tipc

SRG-OS-000480-GPOS-00227
OL 8 must not have the stream control transmission protocol (SCTP) kernel module installed if not required for operational support.
[root@tst-tstla-91 modprobe.d]# cat sctp.conf
install sctp /bin/true
[root@tst-tstla-91 modprobe.d]# cat blacklist.conf
blacklist sctp

SRG-OS-000480-GPOS-00227
OL 8 must not have the Controller Area Network (CAN) kernel module installed if not required for operational support.
[root@tst-tstla-91 modprobe.d]# cat can.conf && cat blacklist.conf
install can /bin/true
blacklist can

SRG-OS-000480-GPOS-00227
OL 8 must not have the asynchronous transfer mode (ATM) kernel module installed if not required for operational support.
[root@tst-tstla-91 modprobe.d]# cat atm.conf
install atm /bin/true
[root@tst-tstla-91 modprobe.d]# cat blacklist.conf
blacklist atm

SRG-OS-000095-GPOS-00049
OL 8 must disable network management of the chrony daemon.
"/etc/chrony.conf" file.
Add the line
cmdport 0
OL 8 must disable the chrony daemon from acting as a server.chrony.conf
Port 0

Configure OL 8 to verify the signature of packages from a repository prior to install by setting the following option in the
"/etc/yum.repos.d/[your_repo_name].repo" file: gpgcheck=1

Configure the "/etc/fstab" to use the "nosuid" option on the /boot directory.
UUID=9129dc4e-95f3-42e2-9423-54af3dd21b96 /boot xfs nosuid,defaults 0 0

SRG-OS-000480-GPOS-00227
Configure OL 8 to disable storing core dumps by adding the following line to a file in the "/etc/sysctl.d" directory: kernel.core_pattern = |/bin/false Remove any configurations that conflict with the above from the following locations: /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf /etc/sysctl.d/*.conf The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command: $ sudo sysctl --system

SRG-OS-000069-GPOS-00037-40

Configure OL 8 to enforce password complexity by requiring that at least one uppercase character be used by setting the "ucredit" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: ucredit = -1 Remove any configurations that conflict with the above value.

Ucredit = -1 , dcredit =-1 , lcredit = -1

Configure OL 8 to require the change of at least four character classes when passwords are changed by setting the "minclass" option. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory: minclass = 4 Remove any configurations that conflict with the above value.

SRG-OS-000206-GPOS-00084
Configure the mode of the "lastlog" command for OL 8 to "0750" with the following command: $ sudo chmod 0750 /usr/bin/lastlog

SRG-OS-000480-GPOS-00227
Configure OL 8 to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin". Add the following line to the top of "/etc/pam.d/postlogin": session required pam_lastlog.so showfailed

SRG-OS-000480-GPOS-00227
Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/sshd" or in the "sshd_config" file used by the system ("/etc/ssh/sshd_config" will be used in the example). Note that this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor. Modify the "PrintLastLog" line in "/etc/ssh/sshd_config" to match the following: PrintLastLog yes The SSH service must be restarted for changes to "sshd_config" to take effect.

Configure OL 8 to audit the execution of the "execve" system call. Add or update the following file system rules to "/etc/audit/rules.d/audit.rules": -a always,exit -F arch=b32 -S execve -C uid!=euid -F key=execpriv -a always,exit -F arch=b64 -S execve -C uid!=euid -F key=execpriv -a always,exit -F arch=b32 -S execve -C gid!=egid -F key=execpriv -a always,exit -F arch=b64 -S execve -C gid!=egid -F key=execpriv The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command: $ sudo service auditd restart

Configure OL 8 to define the default permissions for all authenticated users in such a way that the user can read and modify only their own files. Edit the "UMASK" parameter in the "/etc/login.defs" file to match the example below: UMASK 077

SRG-OS-000004-GPOS-00004
[root@tst-tstla-91 ~]# vi /etc/audit/rules.d/audit.rules
#Configure execution of setattr fseattr
-a always,exit -F arch=b32 -S setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b32 -S setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0 -k perm_mod
-a always,exit -F arch=b64 -S setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0 -k perm_mod

###generate audit records for unix update
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update

#generate audit for setfacl
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F auid!=unset -k perm_chng

#generate audit for rename ulink rmdir
-a always,exit -F arch=b32 -S rename,unlink,rmdir,renameat,unlinkat -F success=1 -F auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S rename,unlink,rmdir,renameat,unlinkat -F success=1 -F auid>=1000 -F auid!=unset -k delete

#generate audit for usermod
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F auid!=unset -k privileged-usermod

#generate audit for chacl
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset -k perm_chng

#generate audit for kmod
-w /usr/bin/kmod -p x -k modules

####
-a always,exit -F arch=b32 -S execve -C uid!=euid -F key=execpriv
-a always,exit -F arch=b64 -S execve -C uid!=euid -F key=execpriv
-a always,exit -F arch=b32 -S execve -C gid!=egid -F key=execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F key=execpriv