

UNCLASSIFIED



Apple macOS 13 (Ventura) Security Technical Implementation Guide

Version: 1

Release: 5

30 Jan 2025

XSL Release 1/25/2022 Sort by: STIGID

Description: This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DOD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Group ID (Vulid): V-257142

Group Title: SRG-OS-000028-GPOS-00009

Rule ID: SV-257142r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000001](#)

Rule Title: The macOS system must be configured to prevent Apple Watch from terminating a session lock.

Vulnerability Discussion: Users must be prompted to enter their passwords when unlocking the screen saver. The screen saver acts as a session lock and prevents unauthorized users from accessing the current user's account.

Check Content:

Verify the macOS system is configured to prevent Apple Watch from terminating a session lock with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowAutoUnlock"
```

```
allowAutoUnlock = 0;
```

If there is no result or "allowAutoUnlock" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to prevent Apple Watch from terminating a session lock by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000056

Group ID (Vulid): V-257143

Group Title: SRG-OS-000028-GPOS-00009

Rule ID: SV-257143r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000002](#)

Rule Title: The macOS system must retain the session lock until the user reestablishes access using established identification and authentication procedures.

Vulnerability Discussion: Users must be prompted to enter their passwords when unlocking the screen saver. The screen saver acts as a session lock and prevents unauthorized users from accessing the current user's account.

Check Content:

Verify the macOS system is configured to prompt users to enter a password to unlock the screen saver with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -w "askForPassword"
```

```
askForPassword = 1;
```

If there is no result, or if "askForPassword" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to prompt users to enter a password to unlock the screen saver by installing the "Login Window Policy" configuration profile.

CCI: CCI-000056

Group ID (Vulid): V-257144

Group Title: SRG-OS-000028-GPOS-00009

Rule ID: SV-257144r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000003](#)

Rule Title: The macOS system must initiate the session lock no more than five seconds after a screen saver is started.

Vulnerability Discussion: A screen saver must be enabled and set to require a password to unlock. An excessive grace period impacts the ability for a session to be truly locked, requiring authentication to unlock.

Check Content:

Verify the macOS system is configured to initiate a session lock within five seconds of the screen saver starting with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "askForPasswordDelay"
```

```
askForPasswordDelay = 5;
```

If there is no result, or if "askForPasswordDelay" is not set to "5" or less, this is a finding.

Fix Text: Configure the macOS system to initiate a session lock within five seconds of the screen saver starting by installing the "Login Window Policy" configuration profile.

CCI: CCI-000056

Group ID (Vulid): V-257145

Group Title: SRG-OS-000029-GPOS-00010

Rule ID: SV-257145r958402_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000004](#)

Rule Title: The macOS system must initiate a session lock after a 15-minute period of inactivity.

Vulnerability Discussion: A screen saver must be enabled and set to require a password to unlock. The timeout must be set to 15 minutes of inactivity. This mitigates the risk that a user might forget to manually lock the screen before stepping away from the computer.

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

Check Content:

Verify the macOS system is configured to initiate the screen saver after 15 minutes of inactivity with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "loginWindowIdleTime"
```

```
loginWindowIdleTime = 900;
```

If there is no result, or if "idleTime" is not set to "900" seconds or less, this is a finding.

Fix Text: Configure the macOS system to initiate the screen saver after 15 minutes of inactivity by installing the "Login Window Policy" configuration profile.

CCI: CCI-000057

Group ID (Vulid): V-257146

Group Title: SRG-OS-000030-GPOS-00011

Rule ID: SV-257146r982194_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000005](#)

Rule Title: The macOS system must be configured to lock the user session when a smart token is removed.

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

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, operating systems must provide users with the ability to manually invoke a session lock so users may secure their session should they need to temporarily vacate the immediate physical vicinity.

Check Content:

Verify the macOS system is configured to lock the user session when a smart token is removed with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "tokenRemovalAction"
```

```
tokenRemovalAction = 1;
```

If there is no result, or if "tokenRemovalAction" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to lock the user session when a smart token is removed by installing the "Smart Card Policy" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the "Smart Card Policy".

CCI: CCI-000058

Group ID (Vulid): V-257147

Group Title: SRG-OS-000031-GPOS-00012

Rule ID: SV-257147r958404_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000006](#)

Rule Title: The macOS system must conceal, via the session lock, information previously visible on the display with a publicly viewable image.

Vulnerability Discussion: A default screen saver must be configured for all users, as the screen saver will act as a session timeout lock for the system and must conceal the contents of the screen from unauthorized users. The screen saver must not display any sensitive information or reveal the contents of the locked session screen. Publicly viewable images can include static or dynamic images such as patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen.

Check Content:

Verify the macOS system is configured with a screen saver with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "moduleName"
```

moduleName = Ventura;

If there is no result or the "moduleName" is undefined, this is a finding.

Fix Text: Configure the macOS system with a screen saver by installing the "Login Window Policy" configuration profile.

CCI: CCI-000060

Group ID (Vulid): V-257148

Group Title: SRG-OS-000031-GPOS-00012

Rule ID: SV-257148r958404_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000007](#)

Rule Title: The macOS system must be configured to disable hot corners.

Vulnerability Discussion: Although hot corners can be used to initiate a session lock or launch useful applications, they can also be configured to disable an automatic session lock from initiating. Such a configuration introduces the risk that a user might forget to manually lock the screen before stepping away from the computer.

Check Content:

Verify the macOS system is configured to disable hot corners with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "wvous"
```

```
"wvous-bl-corner" = 0;
```

```
"wvous-br-corner" = 0;
```

```
"wvous-tl-corner" = 0;
```

```
"wvous-tr-corner" = 0;
```

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

```
"wvous-bl-corner = 0;
```

```
wvous-br-corner = 0;
```

```
wvous-tl-corner = 0;
```

```
wvous-tr-corner = 0;"
```

Fix Text: Configure the macOS system to disable hot corners by installing the "Custom Policy" configuration profile.

CCI: CCI-000060

Group ID (Vulid): V-257150

Group Title: SRG-OS-000002-GPOS-00002

Rule ID: SV-257150r958364_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000012](#)

Rule Title: The macOS system must automatically remove or disable temporary and emergency user accounts after 72 hours.

Vulnerability Discussion: If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be targeted by attackers to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DOD-defined time period of 72 hours.

Emergency administrator accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon/access is not available). Infrequently used accounts also remain available and are not subject to automatic termination dates. However, an emergency administrator account is normally a different account created for use by vendors or system maintainers.

To address access requirements, many operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000002-GPOS-00002, SRG-OS-000123-GPOS-00064

Check Content:

Verify the macOS system is configured with a policy via directory service to disable temporary or emergency accounts after 72 hours by asking the System Administrator (SA) or Information System Security Officer (ISSO).

If a policy is not set by a directory service, a password policy must be set with the "pwpolicy" utility. The variable names may differ depending on how the policy was set.

If temporary or emergency accounts are not defined on the macOS system, this is not applicable.

Verify the macOS system is configured with a policy to disable temporary or emergency accounts after 72 hours with the following command:

```
/usr/bin/sudo /usr/bin/pwpolicy -u username getaccountpolicies | tail -n +2
```

If there is no output and password policy is not controlled by a directory service, this is a finding.

Otherwise, look for the line "<key>policyCategoryAuthentication</key>".

In the array that follows, a <dict> section contains a check <string> that allows users to log in if "policyAttributeCurrentTime" is less than the result of adding "policyAttributeCreationTime" to 72 hours (259299 seconds). The check might use a variable defined in its "policyParameters" section.

If the check does not exist or if the check adds more than 72 hours to "policyAttributeCreationTime", this is a finding.

Fix Text: Configure the macOS system to disable temporary or emergency accounts after 72 hours. This setting may be enforced using local policy or by a directory service.

To set local policy to disable a temporary or emergency user, create a plain text file containing the following:

```
<dict>
  <key>policyCategoryAuthentication</key>
  <array>
    <dict>
      <key>policyContent</key>
      <string>policyAttributeCurrentTime &lt; policyAttributeCreationTime+259299</string>
      <key>policyIdentifier</key>
      <string>Disable Tmp Accounts </string>
    </dict>
  </array>
</dict>
```

After saving the file and exiting to the command prompt, run the following command to load the new policy file, substituting the correct user name in place of "username" and the path to the file in place of "/path/to/file".

```
/usr/bin/sudo /usr/bin/pwpolicy -u username setaccountpolicies /path/to/file
```

CCI: CCI-000016

CCI: CCI-001682

Group ID (Vulid): V-257151

Group Title: SRG-OS-000355-GPOS-00143

Rule ID: SV-257151r1038944_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000014](#)

Rule Title: The macOS system must compare internal information system clocks at least every 24 hours with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet) and/or the Global Positioning System (GPS).

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside of the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Check Content:

Verify the macOS system is configured with the timed service enabled and an authorized time server with the following commands:

```
/usr/bin/sudo /usr/sbin/systemsetup -getusingnetworktime
```

Network Time: On

If "Network Time" is not set to "On", this is a finding.

```
/usr/bin/sudo /usr/sbin/systemsetup -getnetworktimeserver
```

If no time server is configured, or if an unapproved time server is in use, this is a finding.

Fix Text: Configure the macOS system to enable the timed service and set an authorized time server with the following commands:

```
/usr/bin/sudo /usr/sbin/systemsetup -setusingnetworktime on
```

```
/usr/bin/sudo /usr/sbin/systemsetup -setnetworktimeserver "server"
```

CCI: CCI-001891

CCI: CCI-002046

Group ID (Vulid): V-257152

Group Title: SRG-OS-000191-GPOS-00080

Rule ID: SV-257152r982191_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000015](#)

Rule Title: The macOS system must use an Endpoint Security Solution (ESS) and implement all DOD required modules.

Vulnerability Discussion: The macOS system must employ automated mechanisms to determine the state of system components. The DOD requires the installation and use of an approved ESS solution to be implemented on the operating system. For additional information, reference all applicable ESS OPORDs and FRAGOs on SIPRNet.

Check Content:

Verify the macOS system is configured with an approved ESS solution.

If an approved ESS solution is not installed, this is a finding.

Verify that all installed components of the ESS solution are at the DOD-approved minimal version.

If the installed components are not at the DOD-approved minimal versions, this is a finding.

Fix Text: Configure the macOS system with an approved ESS solution and ensure that all components are at least updated to their DOD-approved minimal versions.

CCI: CCI-001233

Group ID (Vulid): V-257153

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257153r991589_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000016](#)

Rule Title: The macOS system must be integrated into a directory services infrastructure.

Vulnerability Discussion: Distinct user account databases on each separate system cause problems with username and password policy enforcement. Most approved directory services infrastructure solutions allow centralized management of users and passwords.

Check Content:

If the macOS system is using a mandatory Smart Card Policy, this requirement is not applicable.

Verify the macOS system is configured to integrate into a directory service with the following command:

```
/usr/bin/dscl localhost -list . | /usr/bin/grep "Active Directory"
```

If no results are returned, this is a finding.

Fix Text: Configure the macOS system to integrate into an existing directory services infrastructure.

CCI: CCI-000366

Group ID (Vulid): V-257154

Group Title: SRG-OS-000329-GPOS-00128

Rule ID: SV-257154r958736_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000022](#)

Rule Title: The macOS system must enforce the limit of three consecutive invalid logon attempts by a user before the user account is locked.

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

Check Content:

Verify the macOS system is configured to enforce the limit of three consecutive invalid logon attempts by a user before the user account is locked with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep  
"maxFailedAttempts\|minutesUntilFailedLoginReset"
```

```
maxFailedAttempts = 3;  
minutesUntilFailedLoginReset = 15;
```

If "maxFailedAttempts" is not set to "3" and "minutesUntilFailedLoginReset" is not set to "15", this is a finding.

Fix Text: Configure the macOS system to enforce the limit of three consecutive invalid logon attempts by a user before the user account is locked by installing the "Passcode Policy" configuration profile or by a directory service.

CCI: CCI-002238

Group ID (Vulid): V-257155

Group Title: SRG-OS-000023-GPOS-00006

Rule ID: SV-257155r958390_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000023](#)

Rule Title: The macOS system must display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system.

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

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

The banner must be formatted in accordance with DTM-08-060.

Check Content:

If SSH is not being used, this is not applicable.

Verify the macOS system is configured to display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system.

Check to see if the operating system has the correct text listed in the "/etc/banner" file with the following command:

```
/usr/bin/more /etc/banner
```

The command must return the following text:

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

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

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

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

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

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

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

If the operating system does not display a logon banner before granting remote access or the banner does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

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

Fix Text: Configure the macOS system to display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system by creating a text file containing the required DOD text.

Name the file "banner" and place it in "/etc/".

CCI: CCI-000048

Group ID (Vulid): V-257156

Group Title: SRG-OS-000023-GPOS-00006

Rule ID: SV-257156r958390_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000024](#)

Rule Title: The macOS system must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via SSH.

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

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

The banner must be formatted in accordance with DTM-08-060.

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

Check Content:

If SSH is not being used, this is not applicable.

Verify the macOS system is configured to display the contents of "/etc/banner" before granting access to the system with the following command:

```
/usr/bin/grep -r Banner /etc/ssh/sshd_config*
```

```
Banner /etc/banner
```

If the sshd Banner configuration option does not point to "/etc/banner", this is a finding.

If conflicting results are returned, this is a finding.

Fix Text: Configure the macOS system to display the contents of "/etc/banner" before granting access to the system with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/^#Banner.*/Banner \etc\banner/' /etc/ssh/sshd_config
```

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-257157

Group Title: SRG-OS-000023-GPOS-00006

Rule ID: SV-257157r958390_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000025](#)

Rule Title: The macOS system must be configured so that any connection to the system must display the Standard Mandatory DOD Notice and Consent Banner before granting GUI access to the system.

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

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

The banner must be formatted in accordance with DTM-08-060.

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

Check Content:

Verify the macOS system is configured to display a policy banner with the following command:

```
/bin/ls -l /Library/Security/PolicyBanner.rtf
```

```
-rw-r--r--@ 1 admin sheel 37 Jan 27 11:18 /Library/Security/PolicyBanner.rtf
```

If "PolicyBanner.rtf" does not exist, this is a finding.

If the permissions for "PolicyBanner.rtf" are not "644", this is a finding.

The banner text of the document must read:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

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

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

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

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

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

If the text is not worded exactly this way, this is a finding.

Fix Text: Configure the macOS system to display a policy banner by creating an RTF file containing the required text. Name the file "PolicyBanner.rtf" and place it in "/Library/Security/".

Update the permissions of the "/Library/Security/PolicyBanner.rtf" file with the following command:

```
/usr/bin/sudo /bin/chmod 644 /Library/Security/PolicyBanner.rtf
```

CCI: CCI-000048

CCI: CCI-000050

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

Group ID (Vulid): V-257158

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257158r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000030](#)

Rule Title: The macOS system must be configured so that log files do not contain access control lists (ACLs).

Vulnerability Discussion: The audit service must be configured to create log files with the correct permissions to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000206-GPOS-00084

Check Content:

Verify the macOS system is configured without ACLs applied to log files with the following command:

```
/usr/bin/sudo /bin/ls -le $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/grep -v current
```

In the output from the above command, ACLs will be listed under any file that may contain them (e.g., "0: group:admin allow list,readattr,readextattr,readsecurity").

If any ACLs exists, this is a finding.

Fix Text: Configure the macOS system so that log files do not contain ACLs with the following command:

```
/usr/bin/sudo /bin/chmod -N [audit log file]
```

CCI: CCI-000162

CCI: CCI-001314

Group ID (Vulid): V-257159

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257159r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000031](#)

Rule Title: The macOS system must be configured so that log folders do not contain access control lists (ACLs).

Vulnerability Discussion: The audit service must be configured to create log folders with the correct permissions to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and users. If log folders are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Check Content:

Verify the macOS system is configured without ACLs applied to log folders with the following command:

```
/usr/bin/sudo /bin/ls -lde $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

In the output from the above command, ACLs will be listed under any folder that may contain them (e.g., "0: group:admin allow list,readattr,readextattr,readsecurity").

If any ACLs exists, this is a finding.

Fix Text: Configure the macOS system so that log folders do not contain ACLs with the following command:

```
/usr/bin/sudo /bin/chmod -N [audit log folder]
```

CCI: CCI-000162

Group ID (Vulid): V-257160

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257160r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000032](#)

Rule Title: The macOS system must be configured with dedicated user accounts to decrypt the hard disk upon startup.

Vulnerability Discussion: When "FileVault" and Multifactor Authentication are configured on the operating system, a dedicated user must be configured to ensure that the implemented Multifactor Authentication rules are enforced. If a dedicated user is not configured to decrypt the hard disk upon startup, the system will allow a user to bypass Multifactor Authentication rules during initial startup and first login.

Check Content:

Verify the macOS system is configured with dedicated user accounts to decrypt the hard disk upon startup with

the following command:

```
/usr/bin/sudo /usr/bin/fdesetup list
```

```
fvuser,85F41F44-22B3-6CB7-85A1-BCC2EA2B887A
```

If any unauthorized users are listed, this is a finding.

Verify that the shell for authorized FileVault users is set to `"/usr/bin/false"` to prevent console logons:

```
/usr/bin/sudo /usr/bin/dscl . read /Users/<FileVault_User> UserShell
```

```
UserShell: /usr/bin/false
```

If the FileVault users' shell is not set to `"/usr/bin/false"`, this is a finding.

Fix Text: Configure the macOS system with a dedicated user account to decrypt the hard disk at startup and disable the logon ability of the newly created user account with the following commands:

```
/usr/bin/sudo /usr/bin/fdesetup add -user <username>
```

```
/usr/bin/sudo /usr/bin/dscl . change /Users/<FileVault_User> UserShell </path/to/current/shell> /usr/bin/false
```

Remove all FileVault logon access from each user account defined on the system that is not a designated FileVault user:

```
/usr/bin/sudo /usr/bin/fdesetup remove -user <username>
```

CCI: CCI-000366

Group ID (Vulid): V-257161

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257161r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000033](#)

Rule Title: The macOS system must be configured to disable password forwarding for FileVault.

Vulnerability Discussion: When "FileVault" and Multifactor Authentication are configured on the operating system, a dedicated user must be configured to ensure that the implemented Multifactor Authentication rules are enforced. If a dedicated user is not configured to decrypt the hard disk upon startup, the system will allow a user to bypass Multifactor Authentication rules during initial startup and first login.

Check Content:

Verify the macOS system is configured to disable password forwarding with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "DisableFDEAutoLogin"
```

```
DisableFDEAutoLogin = 1;
```

If "DisableFDEAutoLogin" is not set to a value of "1", this is a finding.

Fix Text: Configure the macOS system to disable password forwarding by installing the "Smart Card Policy" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the "Smart Card Policy".

CCI: CCI-000366

Group ID (Vulid): V-257162

Group Title: SRG-OS-000163-GPOS-00072

Rule ID: SV-257162r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000051](#)

Rule Title: The macOS system must be configured with the SSH daemon ClientAliveInterval option set to 900 or less.

Vulnerability Discussion: SSH options ClientAliveInterval and ClientAliveCountMax are used in combination to monitor SSH connections. If an SSH client is deemed unresponsive, sshd will terminate the connection. An example would be if a client lost network connectivity the SSH connection to the server would be unresponsive and therefore sshd would terminate the connection after the ClientAliveCountMax and ClientAliveInterval thresholds have been met.

The ClientAliveInterval is a timeout measured in seconds. After which if no data is received from the client, sshd will request a response through the encrypted tunnel from the client. The default is "0", indicating no messages will be sent.

The ClientAliveCountMax is the number of client alive messages that can be sent from the server without receiving a reply from the client. If this threshold is met, sshd will terminate the session. Setting the ClientAliveCountMax to "0" disables connection termination.

Check Content:

If SSH is not being used, this is not applicable.

Verify the macOS system is configured with the SSH daemon "ClientAliveInterval" option set to "900" or less with the following command:

```
/usr/bin/grep -r ^ClientAliveInterval /etc/ssh/sshd_config*
```

If "ClientAliveInterval" is not configured or has a value of "0", this is a finding.

If "ClientAliveInterval" is not "900" or less, this is a finding.

If conflicting results are returned, this is a finding.

Fix Text: Configure the macOS system to set the SSH daemon "ClientAliveInterval" option to "900" with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/.*ClientAliveInterval.*/ClientAliveInterval 900/' /etc/ssh/sshd_config
```

CCI: CCI-001133

Group ID (Vulid): V-257163

Group Title: SRG-OS-000163-GPOS-00072

Rule ID: SV-257163r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000052](#)

Rule Title: The macOS system must be configured with the SSH daemon ClientAliveCountMax option set to 1.

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

SSH options ClientAliveInterval and ClientAliveCountMax are used in combination to monitor SSH connections. If an SSH client is deemed unresponsive, sshd will terminate the connection. An example would be if a client lost network connectivity the SSH connection to the server would be unresponsive and therefore sshd would terminate the connection after the ClientAliveCountMax and ClientAliveInterval thresholds have been met.

The ClientAliveInterval is a timeout measured in seconds. After which if no data is received from the client, sshd will request a response through the encrypted tunnel from the client. The default is 0, indicating no messages will be sent.

The ClientAliveCountMax is the number of client alive messages that can be sent from the server without receiving a reply from the client. If this threshold is met, sshd will terminate the session. Setting the ClientAliveCountMax to 0 disables connection termination.

Check Content:

If SSH is not being used, this is not applicable.

Verify the macOS system is configured with the SSH daemon "ClientAliveCountMax" option set to "1" with the following command:

```
/usr/bin/grep -r ^ClientAliveCountMax /etc/ssh/sshd_config*
```

If the setting is not "ClientAliveCountMax 1", this is a finding.

If conflicting results are returned, this is a finding.

Fix Text: Configure the macOS system to set the SSH daemon "ClientAliveCountMax" option to "1" with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/.*ClientAliveCountMax.*/ClientAliveCountMax 1/' /etc/ssh/sshd_config
```

CCI: CCI-001133

Group ID (Vulid): V-257164

Group Title: SRG-OS-000163-GPOS-00072

Rule ID: SV-257164r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-000053](#)

Rule Title: The macOS system must be configured with the SSH daemon LoginGraceTime set to 30 or less.

Vulnerability Discussion: SSH must be configured to log users out after a 15-minute interval of inactivity and to wait only 30 seconds before timing out logon attempts. Terminating an idle session within a short time reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the

console or console port that has been left unattended. In addition, quickly terminating an idle session or an incomplete logon attempt will also free up resources committed by the managed network element.

Check Content:

If SSH is not being used, this is not applicable.

Verify the macOS system is configured with the SSH daemon "LoginGraceTime" option set to "30" or less with the following command:

```
/usr/bin/grep -r ^LoginGraceTime /etc/ssh/sshd_config*
```

If "LoginGraceTime" is not configured or has a value of "0", this is a finding.

If "LoginGraceTime" is not set to "30" or less, this is a finding.

If conflicting results are returned, this is a finding.

Fix Text: Configure the macOS system to set the SSH daemon "LoginGraceTime" option to "30" with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/.*LoginGraceTime.*/LoginGraceTime 30/' /etc/ssh/sshd_config
```

CCI: CCI-001133

Group ID (Vulid): V-257165

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-257165r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000054](#)

Rule Title: The macOS system must implement approved ciphers within the SSH server configuration to protect the confidentiality of SSH connections.

Vulnerability Discussion: Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to macOS.

For OpenSSH to utilize the Apple Corecrypto FIPS-validated algorithms, a specific configuration is required to leverage the shim implemented by macOS to bypass the non-FIPS validated LibreSSL crypto module packaged with OpenSSH. Information regarding this configuration can be found in the manual page "apple_ssh_and_fips".

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Check Content:

Verify the macOS system is configured to use approved SSH ciphers within the SSH server configuration with the following command:

```
/usr/bin/sudo /usr/sbin/sshd -T | /usr/bin/grep "ciphers"
```

```
ciphers aes128-gcm@openssh.com
```

If any ciphers other than "aes128-gcm@openssh.com" are listed, or the "ciphers" keyword is missing, this is a finding.

Fix Text: Configure the macOS system to use approved SSH ciphers by creating a plain text file in the /private/etc/ssh/ssh_config.d/ directory containing the following:

Ciphers aes128-gcm@openssh.com

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

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-000877

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-257166

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-257166r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000055](#)

Rule Title: The macOS system must implement approved Message Authentication Codes (MACs) within the SSH server configuration.

Vulnerability Discussion: Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to macOS.

For OpenSSH to utilize the Apple Corecrypto FIPS-validated algorithms, a specific configuration is required to leverage the shim implemented by macOS to bypass the non-FIPS validated LibreSSL crypto module packaged with OpenSSH. Information regarding this configuration can be found in the manual page "apple_ssh_and_fips".

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00175

Check Content:

Verify the macOS system is configured to use approved SSH MACs within the SSH server configuration with the following command:

```
/usr/bin/sudo /usr/sbin/sshhd -T | /usr/bin/grep "macs"
```

```
macs hmac-sha2-256
```

If any hashes other than "hmac-sha2-256" are listed, or the "macs" keyword is missing, this is a finding.

Fix Text: Configure the macOS system to use approved SSH MACs by creating a plain text file in the /private/etc/ssh/ssh_config.d/ directory containing the following:

MACs hmac-sha2-256

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

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-000877

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-257167

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-257167r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000056](#)

Rule Title: The macOS system must implement approved Key Exchange Algorithms within the SSH server configuration.

Vulnerability Discussion: Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to macOS.

For OpenSSH to utilize the Apple Corecrypto FIPS-validated algorithms, a specific configuration is required to leverage the shim implemented by macOS to bypass the non-FIPS validated LibreSSL crypto module packaged with OpenSSH. Information regarding this configuration can be found in the manual page "apple_ssh_and_fips".

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00176

Check Content:

Verify the macOS system is configured to use approved SSH Key Exchange Algorithms within the SSH server configuration with the following command:

```
/usr/bin/sudo /usr/sbin/sshd -T | /usr/bin/grep "kexalgorithms"
```

```
kexalgorithms ecdh-sha2-nistp256
```

If any algorithms other than "ecdh-sha2-nistp256" are listed, or the "kexalgorithms" keyword is missing, this is a finding.

Fix Text: Configure the macOS system to use approved SSH Key Exchange Algorithms by creating a plain text file in the /private/etc/ssh/sshd_config.d/ directory containing the following:

KexAlgorithms ecdh-sha2-nistp256

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

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-000877

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-257293

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-257293r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000057](#)

Rule Title: The macOS system must implement approved ciphers within the SSH client configuration to protect the confidentiality of SSH connections.

Vulnerability Discussion: Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to macOS.

For OpenSSH to utilize the Apple Corecrypto FIPS-validated algorithms, a specific configuration is required to leverage the shim implemented by macOS to bypass the non-FIPS validated LibreSSL crypto module packaged with OpenSSH. Information regarding this configuration can be found in the manual page "apple_ssh_and_fips".

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Check Content:

Verify the macOS system is configured to use approved SSH ciphers within the SSH client configuration with the following command:

```
/usr/bin/sudo /usr/bin/grep -ir "ciphers" /etc/ssh/ssh_config*
```

```
/etc/ssh/ssh_config.d/fips_ssh_config:Ciphers aes128-gcm@openssh.com
```

If any ciphers other than "aes128-gcm@openssh.com" are listed, or the "ciphers" keyword is missing, this is a finding.

Fix Text: Configure the macOS system to use approved SSH ciphers by creating a plain text file in the /private/etc/ssh/ssh_config.d/ directory containing the following:

```
Ciphers aes128-gcm@openssh.com
```

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

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-000877

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-257294

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-257294r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000058](#)

Rule Title: The macOS system must implement approved Message Authentication Codes (MACs) within the SSH client configuration.

Vulnerability Discussion: Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to macOS.

For OpenSSH to utilize the Apple Corecrypto FIPS-validated algorithms, a specific configuration is required to leverage the shim implemented by macOS to bypass the non-FIPS validated LibreSSL crypto module packaged with OpenSSH. Information regarding this configuration can be found in the manual page "apple_ssh_and_fips".

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00175

Check Content:

Verify the macOS system is configured to use approved SSH MACs within the SSH client configuration with the following command:

```
/usr/bin/sudo /usr/bin/grep -ir "macs" /etc/ssh/ssh_config*
```

```
/etc/ssh/ssh_config.d/fips_ssh_config:Macs hmac-sha2-256
```

If any hashes other than "hmac-sha2-256" are listed, or the "macs" keyword is missing, this is a finding.

Fix Text: Configure the macOS system to use approved SSH MACs by creating a plain text file in the /private/etc/ssh/ssh_config.d/ directory containing the following:

MACs hmac-sha2-256

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

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-000877

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-257295

Group Title: SRG-OS-000033-GPOS-00014

Rule ID: SV-257295r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-000059](#)

Rule Title: The macOS system must implement approved Key Exchange Algorithms within the SSH client configuration.

Vulnerability Discussion: Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to macOS.

For OpenSSH to utilize the Apple Corecrypto FIPS-validated algorithms, a specific configuration is required to leverage the shim implemented by macOS to bypass the non-FIPS validated LibreSSL crypto module packaged with OpenSSH. Information regarding this configuration can be found in the manual page "apple_ssh_and_fips".

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00176

Check Content:

Verify the macOS system is configured to use approved SSH Key Exchange Algorithms within the SSH client configuration with the following command:

```
/usr/bin/sudo /usr/bin/grep -ir "kexalgorithms" /etc/ssh/ssh_config*
```

```
/etc/ssh/ssh_config.d/fips_ssh_config:KexAlgorithms ecdh-sha2-nistp256
```

If any algorithms other than "ecdh-sha2-nistp256" are listed, or the "kexalgorithms" keyword is missing, this is a finding.

Fix Text: Configure the macOS system to use approved SSH Key Exchange Algorithms by creating a plain text file in the /private/etc/ssh/ssh_config.d/ directory containing the following:

```
KexAlgorithms ecdh-sha2-nistp256
```

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

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-000877

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-257168

Group Title: SRG-OS-000004-GPOS-00004

Rule ID: SV-257168r958368_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001001](#)

Rule Title: The macOS system must generate audit records for all account creations, modifications, disabling, and termination events; privileged activities or other system-level access; all kernel module load, unload, and restart actions; all program initiations; and organizationally defined events for all nonlocal maintenance and diagnostic sessions.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. Audit records can be generated from various components within the information system (e.g., module or policy filter). If events associated with nonlocal administrative access or diagnostic sessions are not logged, a major tool for assessing and investigating attacks would not be available.

This requirement addresses auditing-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems.

Administrative and privileged access, including administrative use of the command line tools "kextload" and "kextunload" and changes to configuration settings, are logged by way of the "ad" flag.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000327-GPOS-00127, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000476-GPOS-00221, SRG-OS-000477-GPOS-00222

Check Content:

Verify the macOS system is configured to audit privileged access with the following command:

```
/usr/bin/sudo /usr/bin/grep ^flags /etc/security/audit_control
```

If "ad" is not listed in the output, this is a finding.

Fix Text: Configure the macOS system to audit privileged access with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak '/^flags/ s/$/,ad/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

A text editor may also be used to implement the required updates to the "/etc/security/audit_control" file.

CCI: CCI-000018

CCI: CCI-000172

CCI: CCI-001403

CCI: CCI-001404

CCI: CCI-001405

CCI: CCI-002234

CCI: CCI-002884

Group ID (Vulid): V-257169

Group Title: SRG-OS-000032-GPOS-00013

Rule ID: SV-257169r958406_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001002](#)

Rule Title: The macOS system must monitor remote access methods and generate audit records when successful/unsuccessful attempts to access/modify privileges occur.

Vulnerability Discussion: Frequently, an attacker that successfully gains access to a system has only gained access to an account with limited privileges, such as a guest account or a service account. The attacker must attempt to change to another user account with normal or elevated privileges to proceed. Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

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

Attempts to log in as another user are logged by way of the "lo" flag.

Satisfies: SRG-OS-000032-GPOS-00013, SRG-OS-000462-GPOS-00206

Check Content:

Verify the macOS system is configured to audit attempts to access/modify privileges with the following command:

```
/usr/bin/sudo /usr/bin/grep ^flags /etc/security/audit_control
```

If "lo" is not listed in the result of the check, this is a finding.

Fix Text: Configure the macOS system to audit attempts to access/modify privileges with the following command:

```
/usr/bin/sudo sed -i.bak '/^flags/ s/$/,lo/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

A text editor may also be used to implement the required updates to the "/etc/security/audit_control" file.

CCI: CCI-000067

CCI: CCI-000172

Group ID (Vulid): V-257170

Group Title: SRG-OS-000037-GPOS-00015

Rule ID: SV-257170r958412_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001003](#)

Rule Title: The macOS system must produce audit records containing information to establish when, where, what type, the source, and the outcome for all DOD-defined auditable events and actions.

Vulnerability Discussion: Without establishing what type of events occurred, when they occurred, and by whom, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

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

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

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00020, SRG-OS-000042-GPOS-00021, SRG-OS-000055-GPOS-00026, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000303-GPOS-00120, SRG-OS-000337-GPOS-00129, SRG-OS-000358-GPOS-00145, SRG-OS-000359-GPOS-00146

Check Content:

Verify the macOS system is configured to enable the auditd service with the following command:

```
/bin/launchctl print-disabled system| /usr/bin/grep com.apple.auditd
```

"com.apple.auditd" => enabled

If the results are not "com.apple.auditd => enabled", this is a finding.

Fix Text: Configure the macOS system to enable the auditd service with the following command:

```
/usr/bin/sudo /bin/launchctl enable system/com.apple.auditd
```

The system may need to be restarted for the update to take effect.

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000159

CCI: CCI-001464

CCI: CCI-001487

CCI: CCI-001889

CCI: CCI-001890

CCI: CCI-001914

CCI: CCI-002130

Group ID (Vulid): V-257171

Group Title: SRG-OS-000047-GPOS-00023

Rule ID: SV-257171r1038966_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001010](#)

Rule Title: The macOS system must shut down by default upon audit failure (unless availability is an overriding concern).

Vulnerability Discussion: The audit service should shut down the computer if it is unable to audit system events. Once audit failure occurs, user and system activity are no longer recorded and malicious activity could go undetected. Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Responses to audit failure depend on the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

(i) If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.

(ii) If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Check Content:

Verify the macOS system is configured to shut down upon audit failure with the following command:

```
/usr/bin/sudo /usr/bin/grep ^policy /etc/security/audit_control | /usr/bin/grep ahlt
```

If there is no result, this is a finding.

Fix Text: Configure the macOS system to shut down upon audit failure by editing the "/etc/security/audit_control" file and updating the policy value to include "ahlt" with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak '/^policy/ s/$/,ahlt/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

CCI: CCI-000140

Group ID (Vulid): V-257172

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257172r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001012](#)

Rule Title: The macOS system must be configured with audit log files owned by root.

Vulnerability Discussion: The audit service must be configured to create log files with the correct ownership to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and users. If log files are set to only be readable and writable by root or administrative users with sudo, the risk is mitigated.

Check Content:

Verify the macOS system is configured with audit log files owned by root with the following command:

```
/usr/bin/sudo /bin/ls -le $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/grep -v current
```

If the files are not owned by root, this is a finding.

Fix Text: Configure the macOS system with audit log files owned by root with the following command:

```
/usr/bin/sudo chown root [audit log file]
```

CCI: CCI-000162

Group ID (Vulid): V-257173

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257173r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001013](#)

Rule Title: The macOS system must be configured with audit log folders owned by root.

Vulnerability Discussion: The audit service must be configured to create log files with the correct ownership to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and about users. If log files are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Check Content:

Verify the macOS system is configured with audit log folders owned by root with the following command:

```
/usr/bin/sudo /bin/ls -lde $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

If the folders are not owned by root, this is a finding.

Fix Text: Configure the macOS system with audit log folders owned by root with the following command:

```
/usr/bin/sudo chown root [audit log folder]
```

CCI: CCI-000162

Group ID (Vulid): V-257174

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257174r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001014](#)

Rule Title: The macOS system must be configured with audit log files group-owned by wheel.

Vulnerability Discussion: The audit service must be configured to create log files with the correct group ownership to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Check Content:

Verify the macOS system is configured with audit log files group-owned by wheel with the following command:

```
/usr/bin/sudo /bin/ls -le $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/grep -v current
```

If the files are not group-owned by wheel, this is a finding.

Fix Text: Configure the macOS system with audit log files group-owned by wheel with the following command:

```
/usr/bin/sudo chgrp wheel [audit log file]
```

CCI: CCI-000162

Group ID (Vulid): V-257175

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257175r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001015](#)

Rule Title: The macOS system must be configured with audit log folders group-owned by wheel.

Vulnerability Discussion: The audit service must be configured to create log files with the correct group ownership to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and about users. If log files are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Check Content:

Verify the macOS system is configured with audit log folders group-owned by wheel with the following command:

```
/usr/bin/sudo /bin/ls -lde $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

If the folders are not group-owned by wheel, this is a finding.

Fix Text: Configure the macOS system with audit log folders group-owned by wheel with the following command:

```
/usr/bin/sudo chgrp wheel [audit log folder]
```

CCI: CCI-000162

Group ID (Vulid): V-257176

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257176r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001016](#)

Rule Title: The macOS system must be configured with audit log files set to mode 440 or less permissive.

Vulnerability Discussion: The audit service must be configured to create log files with the correct permissions to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and about users. If log files are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Check Content:

Verify the macOS system is configured with audit log files set to mode 440 or less with the following command:

```
/usr/bin/sudo /bin/ls -le $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/grep -v current
```

If the files are not mode 440 or less, this is a finding.

Fix Text: Configure the macOS system with audit log files set to mode 440 with the following command:

```
/usr/bin/sudo /bin/chmod 440 [audit log file]
```

CCI: CCI-000162

Group ID (Vulid): V-257177

Group Title: SRG-OS-000057-GPOS-00027

Rule ID: SV-257177r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001017](#)

Rule Title: The macOS system must be configured with audit log folders set to mode 700 or less permissive.

Vulnerability Discussion: The audit service must be configured to create log folders with the correct permissions to prevent normal users from reading audit logs. Audit logs contain sensitive data about the system and users. If log folders are set to be readable and writable only by root or administrative users with sudo, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Check Content:

Verify the macOS system is configured with audit log folders set to mode 700 or less with the following command:

```
/usr/bin/sudo /bin/ls -lde $(/usr/bin/sudo /usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

If the folders are not set to mode 700 or less, this is a finding.

Fix Text: Configure the macOS system with audit log folders set to mode 700 with the following command:

```
/usr/bin/sudo /bin/chmod 700 [audit log folder]
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

Group ID (Vulid): V-257178

Group Title: SRG-OS-000064-GPOS-00033

Rule ID: SV-257178r958446_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001020](#)

Rule Title: The macOS system must audit the enforcement actions used to restrict access associated with changes to the system.

Vulnerability Discussion: By auditing access restriction enforcement, changes to application and OS configuration files can be audited. Without auditing the enforcement of access restrictions, it will be difficult to identify attempted attacks and an audit trail will not be available for forensic investigation.

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. Enforcement action methods may be as simple as denying access to a file based on the application of file permissions (access restriction). Audit items may consist of lists of actions blocked by access restrictions or changes identified after the fact.

Enforcement actions are logged by way of the "fm" flag, which audits permission changes; "-fr" and "-fw", which denote failed attempts to read or write to a file; and "-fd", which audits failed file deletion.

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

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

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000365-GPOS-00152, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209, SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00211, SRG-OS-000468-GPOS-00212, SRG-OS-000474-GPOS-00219

Check Content:

Verify the macOS system is configured to audit enforcement actions with the following command:

```
/usr/bin/sudo /usr/bin/grep ^flags /etc/security/audit_control
```

If "fm", "-fr", "-fw", and "-fd" are not listed in the result of the check, this is a finding.

Fix Text: Configure the macOS system to audit enforcement actions with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak '/^flags/ s/$/,fm,-fr,-fw,-fd/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

A text editor may also be used to implement the required updates to the "/etc/security/audit_control" file.

CCI: CCI-000172

CCI: CCI-001814

Group ID (Vulid): V-257179

Group Title: SRG-OS-000341-GPOS-00132

Rule ID: SV-257179r958752_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-001029](#)

Rule Title: The macOS system must allocate audit record storage capacity to store at least seven days of audit records when audit records are not immediately sent to a central audit record storage facility.

Vulnerability Discussion: The audit service must be configured to require that records are kept for seven days or longer before deletion when there is no central audit record storage facility. When "expire-after" is set to "7d", the audit service will not delete audit logs until the log data is at least seven days old.

Check Content:

Verify the macOS system is configured to store at least seven days of audit records with the following command:

```
/usr/bin/sudo /usr/bin/grep ^expire-after /etc/security/audit_control
```

```
expire-after:7d
```


If "expire-after" is not set to "7d" or greater, this is a finding.

Fix Text: Configure the macOS system to store seven days of audit records with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/. *expire-after:*/expire-after:7d/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

Alternatively, use a text editor to update the "/etc/security/audit_control" file.

CCI: CCI-001849

Group ID (Vulid): V-257180

Group Title: SRG-OS-000343-GPOS-00134

Rule ID: SV-257180r971542_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-001030](#)

Rule Title: The macOS system must provide an immediate warning to the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity.

Vulnerability Discussion: The audit service must be configured to require a minimum percentage of free disk space to run. This ensures that audit will notify the administrator that action is required to free up more disk space for audit logs.

When "minfree" is set to 25 percent, security personnel are notified immediately when the storage volume is 75 percent full and are able to plan for audit record storage capacity expansion.

Check Content:

Verify the macOS system is configured to require a minimum of 25 percent free disk space for audit record storage with the following command:

```
/usr/bin/sudo /usr/bin/grep ^minfree /etc/security/audit_control
```

```
minfree:25
```

If "minfree" is not set to "25", this is a finding.

Fix Text: Configure the macOS system to require 25 percent free disk space for audit record storage with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/. *minfree:*/minfree:25/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

Alternatively, use a text editor to update the "/etc/security/audit_control" file.

CCI: CCI-001855

Group ID (Vulid): V-257181

Group Title: SRG-OS-000344-GPOS-00135

Rule ID: SV-257181r958758_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001031](#)

Rule Title: The macOS system must provide an immediate real-time alert to the System Administrator (SA) and Information System Security Officer (ISSO), at a minimum, of all audit failure events requiring real-time alerts.

Vulnerability Discussion: The audit service must be configured to immediately print messages to the console or email administrator users when an auditing failure occurs. It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Check Content:

Verify the macOS system is configured to print error messages to the console with the following command:

```
/usr/bin/sudo /usr/bin/grep logger /etc/security/audit_warn
```

```
logger -s -p security.warning "audit warning: $type $argument"
```

If the argument "-s" is missing, or if "audit_warn" has not been otherwise modified to print errors to the console or send email alerts to the SA and ISSO, this is a finding.

Fix Text: Configure the macOS system to print error messages to the console with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/logger -p/logger -s -p/' /etc/security/audit_warn; /usr/bin/sudo /usr/sbin/audit -s
```

Alternatively, use a text editor to update the "/etc/security/audit_warn" file.

CCI: CCI-001858

Group ID (Vulid): V-257182

Group Title: SRG-OS-000470-GPOS-00214

Rule ID: SV-257182r991578_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001044](#)

Rule Title: The macOS system must generate audit records for DOD-defined events such as successful/unsuccessful logon attempts, successful/unsuccessful direct access attempts, starting and ending time for user access, and concurrent logons to the same account from different sources.

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

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

Logon events are logged by way of the "aa" flag.

Satisfies: SRG-OS-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218, SRG-OS-000475-GPOS-00220

Check Content:

Verify the macOS system is configured to audit logon events with the following command:

```
/usr/bin/sudo /usr/bin/grep ^flags /etc/security/audit_control
```

If "aa" is not listed in the result of the check, this is a finding.

Fix Text: Configure the macOS system to audit logon events with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak '/^flags/ s/$/,aa/' /etc/security/audit_control; /usr/bin/sudo /usr/sbin/audit -s
```

A text editor may also be used to implement the required updates to the "/etc/security/audit_control" file.

CCI: CCI-000172

Group ID (Vulid): V-257183

Group Title: SRG-OS-000067-GPOS-00035

Rule ID: SV-257183r958450_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001060](#)

Rule Title: The macOS system must accept and verify Personal Identity Verification (PIV) credentials, implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network, and only allow the use of DOD PKI-established certificate authorities for verification of the establishment of protected sessions.

Vulnerability Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DOD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DOD-approved CA, trust of this CA has not been established.

DOD has mandated the use of the CAC to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

The DOD will only accept PKI certificates obtained from a DOD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates.

Satisfies: SRG-OS-000067-GPOS-00035, SRG-OS-000376-GPOS-00161, SRG-OS-000377-GPOS-00162, SRG-OS-000384-GPOS-00167, SRG-OS-000403-GPOS-00182

Check Content:

Verify the macOS system is configured to check the revocation status of user certificates with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "checkCertificateTrust"
```

```
checkCertificateTrust = 1;
```

If there is no result, or if "checkCertificateTrust" is not set to "1" or greater, this is a finding.

Fix Text: Configure the macOS system to check the revocation status of user certificates by installing the "Smart Card Policy" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the "Smart Card Policy".

CCI: CCI-000186

CCI: CCI-001953

CCI: CCI-001954

CCI: CCI-001991

CCI: CCI-002470

Group ID (Vulid): V-257184

Group Title: SRG-OS-000109-GPOS-00056

Rule ID: SV-257184r982205_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-001100](#)

Rule Title: The macOS system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator.

Vulnerability Discussion: Administrator users must never log in directly as root. To assure individual accountability and prevent unauthorized access, logging in as root over a remote connection must be disabled. Administrators must only run commands as root after first authenticating with their individual usernames and passwords.

Check Content:

If SSH is not being used, this is not applicable.

Verify the macOS system is configured to disable root logins over SSH with the following command:

```
/usr/bin/grep -r ^PermitRootLogin /etc/ssh/sshd_config*
```

If there is no result, or the result is set to "yes", this is a finding.

If conflicting results are returned, this is a finding.

Fix Text: Configure the macOS system to disable root logins over SSH with the following command:

```
/usr/bin/sudo /usr/bin/sed -i.bak 's/^[#]*PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
```

CCI: CCI-000770

Group ID (Vulid): V-257185

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257185r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002001](#)

Rule Title: The macOS system must be configured to disable SMB File Sharing unless it is required.

Vulnerability Discussion: File sharing is usually nonessential and must be disabled if not required. Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:

Verify the macOS system is configured to disable the SMB File Sharing service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep com.apple.smbd
```

```
"com.apple.smbd" => disabled
```

If the results are not "com.apple.smbd => disabled" or SMB file sharing has not been documented with the ISSO as an operational requirement, this is a finding.

Fix Text: Configure the macOS system to disable the SMB File Sharing service with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/com.apple.smbd
```

The system may need to be restarted for the update to take effect.

CCI: CCI-000381

Group ID (Vulid): V-257186

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257186r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002003](#)

Rule Title: The macOS system must be configured to disable the Network File System (NFS) daemon unless it is required.

Vulnerability Discussion: If the system does not require access to NFS file shares or is not acting as an NFS server, support for NFS is nonessential and NFS services must be disabled. NFS is a network file system protocol supported by UNIX-like operating systems. Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:

Verify the macOS system is configured to disable the NFS daemon with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep com.apple.nfsd
```

```
"com.apple.nfsd" => disabled
```

If the results are not "com.apple.nfsd => disabled" or the use of NFS has not been documented with the ISSO as an operational requirement, this is a finding.

Fix Text: Configure the macOS system to disable the NFS daemon with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/com.apple.nfsd
```

The system may need to be restarted for the update to take effect.

Group ID (Vulid): V-257187

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257187r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002004](#)

Rule Title: The macOS system must be configured to disable Location Services.

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

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

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

Location Services must be disabled.

Check Content:

Verify the macOS system is configured to disable Location Services with the following command:

```
/usr/bin/sudo /usr/bin/defaults read /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd |  
/usr/bin/grep "LocationServicesEnabled"
```

```
LocationServicesEnabled = 0;
```

If "LocationServicesEnabled" is not set to "0" and the AO has not authorized the use of location services, this is a finding.

Fix Text: Configure the macOS system to disable Location Services with the following command:

```
/usr/bin/sudo /usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd  
LocationServicesEnabled -bool false
```

The system may need to be restarted for the update to take effect.

Group ID (Vulid): V-257188

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257188r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002005](#)

Rule Title: The macOS system must be configured to disable Bonjour multicast advertising.

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

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

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

Bonjour multicast advertising must be disabled on the system.

Check Content:

Verify the macOS system is configured to disable Bonjour multicast advertising with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "NoMulticastAdvertisements"
```

```
NoMulticastAdverstisements = 1;
```

If there is no result, or if "NoMulticastAdvertisements" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable Bonjour multicast advertising by installing the "Custom Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257189

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257189r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002006](#)

Rule Title: The macOS system must be configured to disable the UUCP service.

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

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

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

The system must not have the UUCP service active.

Check Content:

Verify the macOS system is configured to disable the UUCP service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep com.apple.uucp
```

```
"com.apple.uucp" => disabled
```

If the results are not "com.apple.uucp => disabled", this is a finding.

Fix Text: Configure the macOS system to disable the UUCP service with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/com.apple.uucp
```

The system may need to be restarted for the update to take effect.

CCI: CCI-000381

Group ID (Vulid): V-257190

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257190r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002007](#)

Rule Title: The macOS system must be configured to disable Internet Sharing.

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

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

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

Internet Sharing is nonessential and must be disabled.

Check Content:

Verify the macOS system is configured to disable Internet Sharing with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "forceInternetSharingOff"
```

```
forceInternetSharingOff = 1;
```

If there is no result, or if "forceInternetSharingOff" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable Internet Sharing by installing the "Custom Policy" configuration profile.

Group ID (Vulid): V-257191

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257191r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002008](#)

Rule Title: The macOS system must be configured to disable Web Sharing.

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

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

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

Web Sharing is nonessential and must be disabled.

Check Content:

Verify the macOS system is configured to disable Web Sharing with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep org.apache.httpd
```

```
"org.apache.httpd" => disabled
```

If the results are not "org.apache.httpd => disabled", this is a finding.

Fix Text: Configure the macOS system to disable Web Sharing with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/org.apache.httpd
```

The system may need to be restarted for the update to take effect.

Group ID (Vulid): V-257192

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257192r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002009](#)

Rule Title: The macOS system must be configured to disable AirDrop.

Vulnerability Discussion: To prevent unauthorized connection of devices, unauthorized transfer of information,

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

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

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

AirDrop must be disabled.

Note: There is a known bug in the graphical user interface where the user can toggle AirDrop in the UI, which indicates the service has been turned on, but it remains disabled if the Restrictions Profile has been applied.

Check Content:

Verify the macOS system is configured to disable AirDrop with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowAirDrop"
```

```
allowAirDrop = 0;
```

If there is no result, or if "allowAirDrop" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable AirDrop by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257193

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257193r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002012](#)

Rule Title: The macOS system must be configured to disable the iCloud Calendar services.

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

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

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

The Calendar application's connections to Apple's iCloud must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Calendar services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudCalendar"
```

```
allowCloudCalendar = 0;
```

If there is no result, or if "allowCloudCalendar" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Calendar services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257194

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257194r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002013](#)

Rule Title: The macOS system must be configured to disable the iCloud Reminders services.

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

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

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

The Reminder application's connections to Apple's iCloud must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Reminders services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudReminders"
```

```
allowCloudReminders = 0;
```

If there is no result, or if "allowCloudReminders" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Reminders services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257195

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257195r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002014](#)

Rule Title: The macOS system must be configured to disable iCloud Address Book services.

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

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

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

The Address Book(Contacts) application's connections to Apple's iCloud must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Address Book services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudAddressBook"
```

```
allowCloudAddressBook = 0;
```

If there is no result, or if "allowCloudAddressBook" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Address Book services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257196

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257196r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002015](#)

Rule Title: The macOS system must be configured to disable the iCloud Mail services.

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

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

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

The Mail application's connections to Apple's iCloud must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Mail services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudMail"
```

```
allowCloudMail = 0;
```

If there is no result, or if "allowCloudMail" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Mail services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257197

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257197r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002016](#)

Rule Title: The macOS system must be configured to disable the iCloud Notes services.

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

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

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

The Notes application's connections to Apple's iCloud must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Notes services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudNotes"
```

```
allowCloudNotes = 0;
```

If there is no result, or if "allowCloudNotes" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Notes services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257198

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257198r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002017](#)

Rule Title: The macOS system must cover or disable the built-in or attached camera when not in use.

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

Failing to disconnect from collaborative computing devices (i.e., cameras) can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants carry out the disconnect activity without having to go through complex and tedious procedures.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

If the device or operating system does not have a camera installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of the camera is a local AO decision.

This requirement is not applicable to dedicated VTC suites located in approved VTC locations that are centrally managed.

For an external camera, if there is not a method for the operator to manually disconnect camera at the end of collaborative computing sessions, this is a finding.

For a built-in camera, the camera must be protected by a camera cover (e.g., laptop camera cover slide) when not in use. If the built-in camera is not protected with a camera cover, or is not physically disabled, this is a finding.

If the camera is not disconnected, covered, or physically disabled, the following configuration is required:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCamera"
```

```
allowCamera = 0;
```

If the result is "allowCamera = 1" and the collaborative computing device has not been authorized for use, this is a finding.

Fix Text: Configure the macOS system to disable the built-in camera by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257199

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257199r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002020](#)

Rule Title: The macOS system must be configured to disable Siri and dictation.

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

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

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

Siri and dictation must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

To check if Siri and dictation has been disabled, run the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -e "Ironwood Allowed"
```

If the output is not:
"Ironwood Allowed = 0",
this is a finding.

Fix Text: Configure the macOS system to disable Siri and dictation by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257200

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-257200r958480_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002021](#)

Rule Title: The macOS system must be configured to disable sending diagnostic and usage data to Apple.

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

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

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

Sending diagnostic data to Apple must be disabled.

Check Content:

Verify the macOS system is configured to disable sending diagnostic and usage data to Apple with the following command:

```
/usr/bin/sudo /usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep  
"allowDiagnosticSubmission"
```

```
allowDiagnosticSubmission = 0;
```

If there is no result, or if "allowDiagnosticSubmission" is not set to "0", this is a finding.

Alternatively, the settings are found in System Settings >> Privacy & Security >> Privacy >> Analytics & Improvements.

If the box "Share Mac Analytics" is checked, this is a finding.

If the box "Improve Siri & Dictation" is checked, this is a finding.

If the box "Share with app developers" is checked, this is a finding.

Fix Text: Configure the macOS system to disable sending diagnostic and usage data to Apple by installing the "Restrictions Policy" configuration profile.

Alternatively, the settings can be configured in System Settings >> Privacy & Security >> Privacy >> Analytics & Improvements by performing the following:

- Uncheck the box, "Share Mac Analytics".
- Uncheck the box "Improve Siri & Dictation".
- Uncheck the box "Share with app developers".

CCI: CCI-000382

Group ID (Vulid): V-257201

Group Title: SRG-OS-000096-GPOS-00050

Rule ID: SV-257201r958480_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002022](#)

Rule Title: The macOS system must be configured to disable Remote Apple Events.

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

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

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

Remote Apple Events must be disabled.

Check Content:

Verify the macOS system is configured to disable Remote Apple Events with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep com.apple.AEServer
```

```
"com.apple.AEServer" => disabled
```

If the results are not "com.apple.AEServer => disabled", this is a finding.

Fix Text: Configure the macOS system to disable Remote Apple Events with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/com.apple.AEServer
```

The system may need to be restarted for the update to take effect.

CCI: CCI-000382

Group ID (Vulid): V-257202

Group Title: SRG-OS-000370-GPOS-00155

Rule ID: SV-257202r958808_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-002031](#)

Rule Title: The macOS system must be configured to disable the system preference pane for Apple ID.

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

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

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

The Apple ID System Preference Pane must be disabled.

Check Content:

Verify the macOS system is configured to disable access to the Apple ID preference pane with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 6 "DisabledPreferencePanes"
```

If the result is not an array listing "DisabledPreferencePanes" containing "com.apple.preferences.AppleIDPrefPane", this is a finding.

Fix Text: Configure the macOS system to disable access to the Apple ID preference pane by installing the "Restrictions Policy" configuration profile.

CCI: CCI-001774

Group ID (Vulid): V-257203

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257203r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002032](#)

Rule Title: The macOS system must be configured to disable the system preference pane for Internet Accounts.

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

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

Examples of nonessential capabilities include but are not limited to games, software packages, tools, and

demonstration software not related to requirements or providing a wide array of functionality not required for every mission but that cannot be disabled.

The Internet Accounts System Preference Pane must be disabled.

Check Content:

Verify the macOS system is configured to disable access to the Internet Accounts preference pane with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 6 "DisabledPreferencePanes"
```

If the result is not an array listing "DisabledPreferencePanes" containing "com.apple.preferences.internetaccounts", this is a finding.

Fix Text: Configure the macOS system to disable access to the Internet Accounts preference pane by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257204

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257204r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002035](#)

Rule Title: The macOS system must be configured to disable the Cloud Setup services.

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

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

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

Check Content:

Verify the macOS system is configured to disable the Cloud Setup services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SkipCloudSetup"
```

```
SkipCloudSetup = 1;
```

If there is no result, or if "SkipCloudSetup" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable the Cloud Setup services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257205

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257205r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002036](#)

Rule Title: The macOS system must be configured to disable the Privacy Setup services.

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

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

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

Check Content:

Verify the macOS system is configured to disable the Privacy Setup services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SkipPrivacySetup"
```

```
SkipPrivacySetup = 1;
```

If there is no result, or if "SkipPrivacySetup" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable the Privacy Setup services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257206

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257206r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002037](#)

Rule Title: The macOS system must be configured to disable the Cloud Storage Setup services.

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

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

Examples of nonessential capabilities include, but are not limited to, games, software packages, tools, and

demonstration software, not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Check Content:

Verify the macOS system is configured to disable the Cloud Storage Setup services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "Skip iCloud Storage Setup"
```

```
Skip iCloud Storage Setup = 1;
```

If there is no result, or if "Skip iCloud Storage Setup" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable the Cloud Storage Setup services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257207

Group Title: SRG-OS-000074-GPOS-00042

Rule ID: SV-257207r987796_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-002038](#)

Rule Title: The macOS system must be configured to disable the "tftp" service.

Vulnerability Discussion: The "tftp" service must be disabled as it sends all data in a clear-text form that can be easily intercepted and read. The data needs to be protected at all times during transmission, and encryption is the standard method for protecting data in transit.

If the data is not encrypted during transmission, it can be plainly read (i.e., clear text) and easily compromised. Disabling "ftp" is one way to mitigate this risk. Administrators must be instructed to use an alternate service for data transmission that uses encryption, such as SFTP.

Additionally, the "tftp" service uses UDP, which is not secure.

Check Content:

Verify the macOS system is configured to disable the tfptd service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep com.apple.tftpd
```

```
"com.apple.tftpd" => disabled
```

If the results are not "com.apple.tftpd => disabled", this is a finding.

Fix Text: Configure the macOS system to disable the "tftpd" service with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/com.apple.tftpd
```

The system may need to be restarted for the update to take effect.

CCI: CCI-000197

Group ID (Vulid): V-257208

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257208r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002039](#)

Rule Title: The macOS system must be configured to disable the Siri Setup services.

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

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

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

The Siri setup pop-up must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable the Siri Setup services with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SkipSiriSetup"
```

```
SkipSiriSetup = 1;
```

If there is no result, or if "SkipSiriSetup" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable the Siri Setup services by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257209

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257209r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002040](#)

Rule Title: The macOS system must disable iCloud Keychain synchronization.

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

Operating systems can provide a wide variety of functions and services. Some of the functions and services,

provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

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

Keychain synchronization must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Keychain synchronization with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudKeychainSync"
```

```
allowCloudKeychainSync = 0;
```

If there is no result, or if "allowCloudKeychainSync" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Keychain synchronization by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257210

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257210r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002041](#)

Rule Title: The macOS system must disable iCloud Document synchronization.

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

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

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

iCloud Document synchronization must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Document synchronization with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudDocumentSync"  
  
allowCloudDocumentSync = 0;
```

If there is no result, or if "allowCloudDocumentSync" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Document synchronization by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257211

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257211r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002042](#)

Rule Title: The macOS system must disable iCloud Bookmark synchronization.

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

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

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

iCloud Bookmark syncing must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable iCloud Bookmark synchronization with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudBookmarks"  
  
allowCloudBookmarks = 0;
```

If there is no result, or if "allowCloudBookmarks" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Bookmark synchronization by installing the

"Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257212

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257212r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002043](#)

Rule Title: The macOS system must disable the iCloud Photo Library.

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

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

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

The iCloud Photo Library must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable the iCloud Photo Library with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowCloudPhotoLibrary"
```

```
allowCloudPhotoLibrary = 0;
```

If there is no result, or if "allowCloudPhotoLibrary" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to disable the iCloud Photo Library by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257213

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257213r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002050](#)

Rule Title: The macOS system must disable the Screen Sharing feature.

Vulnerability Discussion: The Screen Sharing feature allows remote users to view or control the desktop of the current user. A malicious user can take advantage of screen sharing to gain full access to the system remotely, either with stolen credentials or by guessing the username and password. Disabling Screen Sharing mitigates this risk.

Check Content:

Verify the macOS system is configured to disable the Screen Sharing feature with the following command:

```
/usr/bin/sudo /bin/launchctl print-disabled system | /usr/bin/grep com.apple.screensharing
```

```
"com.apple.screensharing => disabled"
```

If "com.apple.screensharing" is not set to "disabled", this is a finding.

Fix Text: Configure the macOS system to disable the Screen Sharing service with the following command:

```
/usr/bin/sudo /bin/launchctl disable system/com.apple.screensharing
```

The system may need to be restarted for the update to take effect.

CCI: CCI-000366

Group ID (Vulid): V-257214

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257214r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002051](#)

Rule Title: The macOS system must be configured to disable the system preference pane for TouchID and Password.

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

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

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

The TouchID & Password preference pane must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable access to the TouchID & Password preference pane with the

following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 6 "DisabledPreferencePanels"
```

If the result is not an array listing "DisabledPreferencePanels" containing "com.apple.preferences.password", this is a finding.

Fix Text: Configure the macOS system to disable access to the TouchID & Password preference pane by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257215

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257215r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002052](#)

Rule Title: The macOS system must be configured to disable the system preference pane for Wallet and ApplePay.

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

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

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

The Wallet & ApplePay preference pane must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable access to the Wallet & ApplePay preference pane with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 6 "DisabledPreferencePanels"
```

If the return is not two arrays "HiddenPreferencePanels" and "DisabledPreferencePanels", each containing "com.apple.preferences.wallet", this is a finding.

Fix Text: Configure the macOS system to disable access to the Wallet & ApplePay preference pane by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257216

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257216r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002053](#)

Rule Title: The macOS system must be configured to disable the system preference pane for Siri.

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

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

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

The Siri preference pane must be disabled.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

Check Content:

Verify the macOS system is configured to disable access to the Siri preference pane with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 6 "DisabledPreferencePanels"
```

If the result is not an array listing "DisabledPreferencePanels" containing "com.apple.preference.speech", this is a finding.

Fix Text: Configure the macOS system to disable access to the Siri preference pane by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

CCI: CCI-001774

Group ID (Vulid): V-257217

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257217r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002060](#)

Rule Title: The macOS system must only allow applications with a valid digital signature to run.

Vulnerability Discussion: Gatekeeper settings must be configured correctly to only allow the system to run

applications signed with a valid Apple Developer ID code. Administrator users will still have the option to override these settings on a per-app basis. Gatekeeper is a security feature that ensures that applications must be digitally signed by an Apple-issued certificate to run. Digital signatures allow the macOS host to verify that the application has not been modified by a malicious third party.

Check Content:

Verify the macOS system is configured to only allow applications with a valid digital signature with the following commands:

```
/usr/sbin/system_profiler SPApplicationsDataType | /usr/bin/grep -B 3 -A 4 -e "Obtained from: Unknown" |  
/usr/bin/grep -v -e "Location: /Library/Application Support/Script Editor/Templates" -e "Location:  
/System/Library/" | /usr/bin/awk -F "Location: " '{print $2}' | /usr/bin/sort -u
```

If any results are returned and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify only applications with a valid digital signature are allowed to run:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -E "(EnableAssessment |  
AllowIdentifiedDevelopers)"
```

If the result is not as follows, this is a finding.

```
"AllowIdentifiedDevelopers = 1;  
EnableAssessment = 1;"
```

Fix Text: Configure the macOS system to only allow applications with a valid digital signature by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257218

Group Title: SRG-OS-000379-GPOS-00164

Rule ID: SV-257218r971545_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-002062](#)

Rule Title: The macOS system must be configured with Bluetooth turned off unless approved by the organization.

Vulnerability Discussion: Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read, altered, or used to compromise the operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with an operating system. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR keyboards, mice, and pointing devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DOD requirements for wireless data transmission and be approved for use by the AO. Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by

physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

Satisfies: SRG-OS-000379-GPOS-00164, SRG-OS-000481-GPOS-00481

Check Content:

Verify the macOS system is configured to disable Bluetooth with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "DisableBluetooth"
```

```
DisableBluetooth = 1;
```

If the result is not "DisableBluetooth = 1" and the use of Bluetooth has not been documented with the ISSO as an operational requirement, this is a finding.

Verify the macOS system is configured to disable access to the Bluetooth preference pane with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 6 "DisabledPreferencePanes"
```

If the result is not an array listing "DisabledPreferencePanes" containing "com.apple.preferences.Bluetooth" and the use of Bluetooth has not been documented with the ISSO as an operational requirement, this is a finding.

Fix Text: Configure the macOS system to disable Bluetooth and disable access to the Bluetooth preference pane by installing the "Custom Policy" and "Restrictions Policy" configuration profiles.

CCI: CCI-001967

CCI: CCI-002418

Group ID (Vulid): V-257219

Group Title: SRG-OS-000364-GPOS-00151

Rule ID: SV-257219r958796_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-002063](#)

Rule Title: The macOS system must disable the guest account.

Vulnerability Discussion: Failure to provide logical access restrictions associated with changes to system configuration may have significant effects on the overall security of the system.

When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the operating system can have significant effects on the overall security of the system.

Accordingly, only qualified and authorized individuals must be allowed to obtain access to operating system components for the purposes of initiating changes, including upgrades and modifications.

Logical access restrictions include, for example, controls that restrict access to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making

unauthorized changes easy to discover).

Check Content:

Verify the macOS system is configured to disable the guest account with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "GuestAccount"
```

```
DisableGuestAccount = 1;  
EnableGuestAccount = 0;
```

If the result are not "DisableGuestAccount = 1" and "EnableGuestAccount = 0", this is a finding.

Fix Text: Configure the macOS system to disable the guest account by installing the "Login Window Policy" configuration profile.

CCI: CCI-001813

Group ID (Vulid): V-257220

Group Title: SRG-OS-000366-GPOS-00153

Rule ID: SV-257220r982212_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-002064](#)

Rule Title: The macOS system must have the security assessment policy subsystem enabled.

Vulnerability Discussion: Any changes to the hardware, software, and/or firmware components of the information system and/or application can potentially have significant effects on the overall security of the system.

Accordingly, software defined by the organization as critical must be signed with a certificate that is recognized and approved by the organization.

Check Content:

Verify the macOS system is configured with the security assessment policy subsystem enabled with the following command:

```
/usr/sbin/spctl --status
```

```
assessments enabled
```

If "assessments enabled" is not returned, this is a finding.

Fix Text: Configure the macOS system to enable the security assessment policy subsystem by installing the "Custom Policy" configuration profile.

CCI: CCI-001749

Group ID (Vulid): V-257221

Group Title: SRG-OS-000480-GPOS-00229

Rule ID: SV-257221r991591_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002066](#)

Rule Title: The macOS system must not allow an unattended or automatic logon to the system.

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

Check Content:

Verify the macOS system is configured to not allow automatic logon with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "DisableAutoLoginClient"
```

```
"com.apple.login.mcx.DisableAutoLoginClient" = 1;
```

If "com.apple.login.mcx.DisableAutoLoginClient" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to not allow automatic login by installing the "Login Window Policy" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257222

Group Title: SRG-OS-000480-GPOS-00228

Rule ID: SV-257222r991590_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002068](#)

Rule Title: The macOS system must set permissions on user home directories to prevent users from having access to read or modify another user's files.

Vulnerability Discussion: Configuring the operating system to use the most restrictive permissions possible for user home directories helps to protect against inadvertent disclosures.

Satisfies: SRG-OS-000480-GPOS-00228, SRG-OS-000480-GPOS-00230

Check Content:

Verify the macOS system is configured so that permissions are set correctly on user home directories with the following commands:

```
/bin/ls -le /Users
```

This command will return a listing of the permissions of the root of every user account configured on the system. For each of the users, the permissions must be "drwxr-xr-x+", with the user listed as the owner and the group listed as "staff". The plus(+) sign indicates an associated Access Control List, which must be:

```
0: group:everyone deny delete
```

For every authorized user account, also run the following command:

```
/usr/bin/sudo /bin/ls -le /Users/userid, where userid is an existing user.
```

This command will return the permissions of all the objects under the users' home directory. The permissions for each of the subdirectories must be:

```
drwx-----+
```

```
0: group:everyone deny delete
```

The exception is the "Public" directory, whose permissions must match the following:

```
drwxr-xr-x+
```


0: group:everyone deny delete

If the permissions returned by either of these checks differ from what is shown, this is a finding.

Fix Text: Configure the macOS system to set the appropriate permissions for each user on the system with the following command:

`/usr/sbin/diskutil resetUserPermissions / DeviceNode UID`, where "DeviceNode UID" is the ID number for the user whose home directory permissions need to be repaired.

CCI: CCI-000366

Group ID (Vulid): V-257776

Group Title: SRG-OS-000324-GPOS-00125

Rule ID: SV-257776r958726_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-002069](#)

Rule Title: The macOS system must prevent nonprivileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Vulnerability Discussion: Preventing nonprivileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

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

Check Content:

Verify the macOS system is configured to require authentication to access all system-level preference panes with the following commands:

```
/usr/bin/sudo /usr/bin/security authorizationdb read system.preferences | /usr/bin/grep -A1 shared
```

```
<key>shared</key>
```

```
<false/>
```

If the "shared" key is not set to "false", this is a finding.

Fix Text: Configure the macOS system to require authentication to access all system-level preference panes with the following actions:

Copy the authorization database to a file:

```
/usr/bin/sudo /usr/bin/security authorizationdb read system.preferences > ~/Desktop/authdb.txt
```

Edit the "shared" section of the file:

```
<key>shared</key>
```

```
<false/>
```

Reload the authorization database:

```
/usr/bin/sudo /usr/bin/security authorizationdb write system.preferences < ~/Desktop/authdb.txt
```

CCI: CCI-002235

Group ID (Vulid): V-257224
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-257224r991589_rule
Severity: CAT I
Rule Version (STIG-ID): [APPL-13-002070](#)
Rule Title: The macOS system must use an approved antivirus program.

Vulnerability Discussion: An approved antivirus product must be installed and configured to run.

Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the operating system.

Check Content:

Verify the macOS system is configured to enforce installation of XProtect Remediator and Gatekeeper updates automatically with the following command:

```
/usr/bin/defaults read /Library/Preferences/com.apple.SoftwareUpdate.plist | /usr/bin/grep "ConfigDataInstall"
```

```
ConfigDataInstall = 1;
```

If the XProtect service is being used and "ConfigDataInstall" is not set to "1", this is a finding.

If XProtect is not active on the system, ask the system administrator (SA) or information system security officer (ISSO) if an approved antivirus solution is loaded on the system. The antivirus solution may be bundled with an approved host-based security solution.

If no local antivirus solution is installed on the system, this is a finding.

Fix Text: Configure the macOS system to automatically update XProtect by installing the "Restrictions Policy" configuration profile.

If XProtect is not being used, install an approved antivirus solution on the system.

CCI: CCI-000366

Group ID (Vulid): V-257225
Group Title: SRG-OS-000066-GPOS-00034
Rule ID: SV-257225r958448_rule
Severity: CAT I
Rule Version (STIG-ID): [APPL-13-003001](#)
Rule Title: The macOS system must issue or obtain public key certificates under an appropriate certificate policy from an approved service provider.

Vulnerability Discussion: DOD-approved certificates must be installed to the System Keychain so they will be available to all users.

For user certificates, each organization obtains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include

certificates related to internal system operations; for example, application-specific time services. Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000478-GPOS-00223

Check Content:

Verify the macOS system is configured with approved DOD certificates with the following command:

```
/usr/bin/sudo /usr/bin/security dump-keychain | /usr/bin/grep labl | /usr/bin/awk -F" '{ print $4 }'
```

If this list contains unapproved certificates, this is a finding.

Fix Text: Configure the macOS system with approved DOD certificates from the appropriate authority. Use Keychain Access from "/Applications/Utilities" to add certificates to the System Keychain or build a certificate root trust payload as described in the supplemental documentation supplied in this STIG package.

CCI: CCI-000185

CCI: CCI-002450

Group ID (Vulid): V-257226

Group Title: SRG-OS-000071-GPOS-00039

Rule ID: SV-257226r982197_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003007](#)

Rule Title: The macOS system must enforce password complexity by requiring that at least one numeric character be used.

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

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

Check Content:

Verify the macOS system is configured to require at least one numeric character in password complexity with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "requireAlphanumeric"
```

```
requireAlphanumeric = 1;
```

If the result is not "requireAlphanumeric = 1", this is a finding.

Fix Text: Configure the macOS system to require at least one numeric character in password complexity by installing the "Passcode Policy" configuration profile.

CCI: CCI-000194

Group ID (Vulid): V-257227

Group Title: SRG-OS-000076-GPOS-00044

Rule ID: SV-257227r1038967_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003008](#)

Rule Title: The macOS system must enforce a 60-day maximum password lifetime restriction.

Vulnerability Discussion: Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically.

One method of minimizing this risk is to use complex passwords and periodically change them. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Check Content:

Verify the macOS system is configured to enforce a 60-day maximum password lifetime with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "maxPINAgeInDays"
```

```
maxPINAgeInDays = 60;
```

If "maxPINAgeInDays" is set a value greater than "60", this is a finding.

Fix Text: Configure the macOS system to require the enforcement of a 60-day maximum password lifetime by installing the "Passcode Policy" configuration profile.

CCI: CCI-000199

Group ID (Vulid): V-257228

Group Title: SRG-OS-000077-GPOS-00045

Rule ID: SV-257228r982201_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003009](#)

Rule Title: The macOS system must prohibit password reuse for a minimum of five generations.

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

Check Content:

Verify the macOS system is configured to prohibit password reuse for a minimum of five generations with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "pinHistory"
```

```
pinHistory = 5;
```

If "pinHistory" is not set to "5" or greater, this is a finding.

Fix Text: Configure the macOS system to prohibit password reuse for five generations by installing the "Passcode Policy" configuration profile.

CCI: CCI-000200

Group ID (Vulid): V-257229

Group Title: SRG-OS-000078-GPOS-00046

Rule ID: SV-257229r982202_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003010](#)

Rule Title: The macOS system must enforce a minimum 15-character password length.

Vulnerability Discussion: The minimum password length must be set to 15 characters. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. The use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Check Content:

Verify the macOS system is configured to enforce a minimum 15-character password length with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "minLength"
```

```
minLength = 15;
```

If "minLength" is not set to "15", this is a finding.

Fix Text: Configure the macOS system to enforce a 15-character password length by installing the "Passcode Policy" configuration profile.

CCI: CCI-000205

Group ID (Vulid): V-257230

Group Title: SRG-OS-000266-GPOS-00101

Rule ID: SV-257230r991561_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003011](#)

Rule Title: The macOS system must enforce password complexity by requiring that at least one special character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity or strength is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised. Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ *.

Check Content:

Verify the macOS system is configured to enforce at least one special character of password complexity with the

following commands:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "minComplexChars"
```

```
minComplexChar = 1;
```

If "minComplexChars" is not set to "1", this is a finding.

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowSimple"
```

```
allowSimple = 0;
```

If "allowSimple" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to enforce at least one special character of password complexity by installing the "Passcode Policy" configuration profile.

CCI: CCI-001619

Group ID (Vulid): V-257231

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257231r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003012](#)

Rule Title: The macOS system must be configured to prevent displaying password hints.

Vulnerability Discussion: Password hints leak information about passwords in use and can lead to loss of confidentiality.

Check Content:

Verify the macOS system is configured to prevent displaying passwords hints with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "RetriesUntilHint"
```

```
RetriesUntilHint = 0;
```

If "RetriesUntilHint" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to prevent displaying password hints by installing the "Login Window Policy" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257232

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257232r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003013](#)

Rule Title: The macOS system must be configured with a firmware password to prevent access to single user mode and booting from alternative media.

Vulnerability Discussion: Single user mode and the boot picker, as well as numerous other tools, are available

on macOS through booting while holding the "Option" key down. Setting a firmware password restricts access to these tools.

Check Content:

For Apple Silicon-based systems, this is not applicable.

Verify the macOS system is configured with a firmware password with the following command:

```
/usr/bin/sudo /usr/sbin/firmwarepasswd -check
```

Password Enabled: Yes

If "Password Enabled" is not set to "Yes", this is a finding.

Fix Text: Configure the macOS system with a firmware password with the following command:

```
/usr/bin/sudo /usr/sbin/firmwarepasswd -setpasswd
```

Note: If firmware password or passcode is forgotten, the only way to reset the forgotten password is through a machine-specific binary generated and provided by Apple. Users must schedule a support call and provide proof of purchase before the firmware binary will be generated.

CCI: CCI-000366

Group ID (Vulid): V-257233

Group Title: SRG-OS-000068-GPOS-00036

Rule ID: SV-257233r958452_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-003020](#)

Rule Title: The macOS system must use multifactor authentication for local access to privileged and nonprivileged accounts.

Vulnerability Discussion: Without the use of multifactor authentication, the ease of access to privileged and nonprivileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

- 1) something a user knows (e.g., password/PIN);
- 2) something a user has (e.g., cryptographic identification device, token); and
- 3) something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Local access is defined as access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

The DOD CAC with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000068-GPOS-00036, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Check Content:

Verify the macOS system is configured to enforce multifactor authentication with the following commands:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "enforceSmartCard"
```

```
enforceSmartCard = 1;
```

If "enforceSmartCard" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to enforce multifactor authentication by installing the "Smart Card Policy" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the "Smart Card Policy".

CCI: CCI-000187

CCI: CCI-000767

CCI: CCI-000768

Group ID (Vulid): V-257234

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257234r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003050](#)

Rule Title: The macOS system must be configured so that the login command requires smart card authentication.

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

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

Check Content:

For systems that are not using smart card authentication, this requirements is not applicable.

Verify the macOS system is configured to require smart card authentication for the login command with the following command:

```
/bin/cat /etc/pam.d/login
```

If the text that returns does not include the line "auth sufficient pam_smartcard.so" at the TOP of the listing and "auth required pam_deny.so" as the last entry of the auth management group, this is a finding.

Fix Text: Configure the macOS system to require smart card authentication for the login command with the following procedure:


```
/usr/bin/sudo /bin/cp /etc/pam.d/login /etc/pam.d/login_backup_`date "+%Y-%m-%d_%H:%M"`
```

Replace the contents of "/etc/pam.d/login" with the following:

```
# login: auth account password session
auth sufficient pam_smartcard.so
auth optional pam_krb5.so use_kcminit
auth optional pam_ntlm.so try_first_pass
auth optional pam_mount.so try_first_pass
auth required pam_opendirectory.so try_first_pass
auth required pam_deny.so
account required pam_nologin.so
account required pam_opendirectory.so
password required pam_opendirectory.so
session required pam_launchd.so
session required pam_uwtmp.so
session optional pam_mount.so
```

CCI: CCI-000366

Group ID (Vulid): V-257235

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257235r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003051](#)

Rule Title: The macOS system must be configured so that the su command requires smart card authentication.

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

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

Check Content:

For systems that are not using smart card authentication, this requirement is not applicable.

Verify the macOS system is configured to require smart card authentication for the "su" command with the following command:

```
/bin/cat /etc/pam.d/su
```

If the text that returns does not include the line, "auth sufficient pam_smartcard.so" at the TOP of the listing and the next line is not "auth required pam_rootok.so", this is a finding.

Fix Text: Configure the macOS system to require smart card authentication for the su command with the following procedure:

```
/usr/bin/sudo /bin/cp /etc/pam.d/su /etc/pam.d/su_backup_`date "+%Y-%m-%d_%H:%M"`
```

Replace the contents of "/etc/pam.d/su" with the following:

```
# su: auth account session
auth sufficient pam_smartcard.so
auth required pam_rootok.so
account required pam_group.so no_warn group=admin,wheel ruser root_only fail_safe
account required pam_opendirectory.so no_check_shell
password required pam_opendirectory.so
session required pam_launchd.so
```

CCI: CCI-000366

Group ID (Vulid): V-257236

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257236r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-003052](#)

Rule Title: The macOS system must be configured so that the sudo command requires smart card authentication.

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

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

Check Content:

For systems that are not using smart card authentication, this requirement is not applicable.

Verify the macOS system is configured to require smart card authentication for the "sudo" command with the following command:

```
/bin/cat /etc/pam.d/sudo
```

If the text that returns does not include the line, "auth sufficient pam_smartcard.so" at the top of the listing and "auth required pam_deny.so" as the last entry of the auth management group, this is a finding.

Fix Text: Configure the macOS system to require smart card authentication for the sudo command with the following procedure:

```
/usr/bin/sudo /bin/cp /etc/pam.d/login /etc/pam.d/sudo_backup_`date "+%Y-%m-%d_%H:%M"`
```

Replace the contents of "/etc/pam.d/sudo" with the following:

```
# sudo: auth account password session
```

auth sufficient pam_smartcard.so
auth required pam_opendirectory.so
auth required pam_deny.so
account required pam_permit.so
password required pam_deny.so
session required pam_permit.so

CCI: CCI-000366

Group ID (Vulid): V-257237

Group Title: SRG-OS-000206-GPOS-00084

Rule ID: SV-257237r958566_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-004001](#)

Rule Title: The macOS system must be configured with system log files owned by root and group-owned by wheel or admin.

Vulnerability Discussion: System logs must only be readable by root or admin users. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct owner mitigates this risk.

Some system log files are controlled by "newsyslog" and "aslmanager".

Check Content:

Verify the macOS system is configured with system log files owned by root or a service account and group-owned by wheel or admin with the commands below.

These commands must be run from inside "/var/log".

```
/usr/bin/sudo /usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null
```

```
/usr/bin/sudo /usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null
```

If there are any system log files that are not owned by "root" or a service account and group-owned by "wheel" or "admin", this is a finding.

Fix Text: Configure the macOS system with system log files owned by root or a service account and group-owned by wheel or admin with the following command:

```
/usr/bin/sudo chown root:wheel [log file]
```

Alternatively, if the file is managed by "newsyslog", find the configuration line in the directory "/etc/newsyslog.d/" or the file "/etc/newsyslog.conf" and ensure the owner:group column is set to "root:wheel" or the appropriate service account and group.

If the file is managed by "aslmanager", find the configuration line in the directory "/etc/asl/" or the file "/etc/asl.conf" and ensure that "uid" and "gid" options are set to a service account and group, respectively.

CCI: CCI-001314

Group ID (Vulid): V-257238

Group Title: SRG-OS-000206-GPOS-00084

Rule ID: SV-257238r958566_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-004002](#)

Rule Title: The macOS system must be configured with system log files set to mode 640 or less permissive.

Vulnerability Discussion: System logs must only be readable by root or admin users. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

Check Content:

Verify the macOS system is configured with system log files set to mode 640 or less with the commands below.

These commands must be run from inside `"/var/log"`.

```
/usr/bin/sudo /usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null
```

```
/usr/bin/sudo /usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null
```

If the permissions on log files are not "640" or less permissive, this is a finding.

Fix Text: Configure the macOS system with system log files set to mode 640 with the following command:

```
/usr/bin/sudo chmod 640 [log file]
```

Alternatively, if the file is managed by "newsyslog", find the configuration line in the directory `"/etc/newsyslog.d/"` or the file `"/etc/newsyslog.conf"` and edit the mode column to be "640". Or, if the file is managed by "aslmanager", find the configuration line in the directory `"/etc/asl/"` or the file `"/etc/asl.conf"` and add or edit the mode option to be "mode=0640".

CCI: CCI-001314

Group ID (Vulid): V-257239

Group Title: SRG-OS-000373-GPOS-00156

Rule ID: SV-257239r1050789_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-004022](#)

Rule Title: The macOS system must require users to reauthenticate for privilege escalation when using the "sudo" command.

Vulnerability Discussion: Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

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

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

Check Content:

Verify the macOS system requires reauthentication when using the "sudo" command to elevate privileges with the following command:

```
/usr/bin/sudo /usr/bin/grep -r "timestamp_timeout" /etc/sudoers*
```

```
/etc/sudoers.d/<customfile>:Defaults timestamp_timeout=0
```

If conflicting results are returned, this is a finding.

If "timestamp_timeout" is set to a negative number, is commented out, or no results are returned, this is a finding.

Fix Text: Configure the macOS system to require reauthentication when using the "sudo" command by creating a plain text file in the /private/etc/sudoers.d/ directory containing the following:

```
Defaults timestamp_timeout=0
```

CCI: CCI-002038

Group ID (Vulid): V-257240

Group Title: SRG-OS-000051-GPOS-00024

Rule ID: SV-257240r958428_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-005001](#)

Rule Title: The macOS system must enable System Integrity Protection.

Vulnerability Discussion: System Integrity Protection (SIP) is vital to the protection of the integrity of macOS. SIP restricts what actions can be performed by administrative users, including root, against protected parts of the operating system. SIP protects all system binaries, including audit tools, from unauthorized access by preventing the modification or deletion of system binaries, or the changing of the permissions associated with those binaries. SIP limits the privileges to change software resident within software libraries to processes that have signed by Apple and have special entitlements to write to system files, such as Apple software updates and Apple installers. By protecting audit binaries, SIP ensures the presence of an audit record generation capability for DOD-defined auditable events for all operating system components and supports on-demand and after-the-fact reporting requirements.

The XProtect program is part of the SIP component and is integral to protecting the operating system from malware and malicious code.

Satisfies: SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000062-GPOS-00031, SRG-OS-000122-GPOS-00063, SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000259-GPOS-00100, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142

Check Content:

Verify the macOS system is configured to enable System Integrity Protection with the following command:

```
/usr/bin/csrutil status
```

System Integrity Protection status: enabled.

If the "System Integrity Protection" is not set to "enabled", this is a finding.

Fix Text: Configure the macOS system to enable "System Integrity Protection" by booting into "Recovery" mode, then launch "Terminal" from the "Utilities" menu, and run the following command:

/usr/bin/csrutil enable

CCI: CCI-000154

CCI: CCI-000158

CCI: CCI-000169

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-001499

CCI: CCI-001875

CCI: CCI-001876

CCI: CCI-001877

CCI: CCI-001878

CCI: CCI-001879

CCI: CCI-001880

CCI: CCI-001881

CCI: CCI-001882

Group ID (Vulid): V-257241

Group Title: SRG-OS-000185-GPOS-00079

Rule ID: SV-257241r958552_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-005020](#)

Rule Title: The macOS system must implement cryptographic mechanisms to protect the confidentiality and integrity of all information at rest.

Vulnerability Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive) within an organizational information system. Mobile devices,

laptops, desktops, and storage devices can be lost or stolen, and the contents of their data storage (e.g., hard drives and nonvolatile memory) can be read, copied, or altered. By encrypting the system hard drive, the confidentiality and integrity of any data stored on the system is ensured. FileVault Disk Encryption mitigates this risk.

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Check Content:

Verify the macOS system is configured to enable "FileVault" with the following command:

```
/usr/bin/fdesetup status
```

If "FileVault" is "Off" and the device is a mobile device or the organization has determined that the drive must encrypt data at rest, this is a finding.

Fix Text: Configure the macOS system to enable "FileVault" by opening System Settings >> Privacy & Security >> Security and navigate to the "FileVault" section. Use this panel to configure full-disk encryption.

Alternatively, from the command line, run the following command to enable "FileVault":

```
/usr/bin/sudo /usr/bin/fdesetup enable
```

After "FileVault" is initially set up, additional users can be added.

CCI: CCI-001199

CCI: CCI-002475

CCI: CCI-002476

Group ID (Vulid): V-257242

Group Title: SRG-OS-000480-GPOS-00232

Rule ID: SV-257242r991593_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005050](#)

Rule Title: The macOS Application Firewall must be enabled.

Vulnerability Discussion: Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Check Content:

Verify the macOS system is configured to enable the built-in firewall with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "EnableFirewall\|EnableStealthMode"
```

```
EnableFirewall = 1;
```

```
EnableStealthMode = 1;
```

If "EnableFirewall" and "EnableStealthMode" are not set to "1", this is a finding.

Fix Text: Configure the macOS system to enable the built-in firewall by installing the "Restrictions Policy"

configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257243

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257243r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005051](#)

Rule Title: The macOS system must restrict the ability of individuals to use USB storage devices.

Vulnerability Discussion: External writeable media devices must be disabled for users. External USB devices are a potential vector for malware and can be used to exfiltrate sensitive data if an approved data-loss prevention (DLP) solution is not installed.

Check Content:

Verify the macOS system is configured to disable USB storage devices with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep -A 32 "mount-controls"
```

```
bd = (  
  "read-only"  
);  
blankbd = (  
  deny,  
  eject  
);  
blankcd = (  
  deny,  
  eject  
);  
blankdvd = (  
  deny,  
  eject  
);  
cd = (  
  "read-only"  
);  
"disk-image" = (  
  "read-only"  
);  
dvd = (  
  "read-only"  
);  
dvdram = (  
  deny,  
  eject  
);  
"harddisk-external" = (  
  deny,  
  eject  
);
```


If the result does not match the output above and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Fix Text: Configure the macOS system to disable USB storage devices by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257244

Group Title: SRG-OS-000480-GPOS-00229

Rule ID: SV-257244r991591_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005052](#)

Rule Title: The macOS system logon window must be configured to prompt for username and password.

Vulnerability Discussion: The logon window must be configured to prompt all users for both a username and a password. By default, the system displays a list of known users at the logon screen. This gives an advantage to an attacker with physical access to the system, as the attacker would only have to guess the password for one of the listed accounts.

Check Content:

Verify the macOS system is configured to prompt for username and password at the logon window with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SHOWFULLNAME"
```

```
SHOWFULLNAME = 1;
```

If "SHOWFULLNAME" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to prompt for username and password at the logon window by installing the "Login Window Policy" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257245

Group Title: SRG-OS-000480-GPOS-00227

Rule ID: SV-257245r991589_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-005053](#)

Rule Title: The macOS system must restrict the ability of individuals to write to external optical media.

Vulnerability Discussion: External writeable media devices must be disabled for users. External optical media devices can be used to exfiltrate sensitive data if an approved data-loss prevention (DLP) solution is not installed.

Check Content:

Verify the macOS system is configured to disable writing to external optical media devices with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "BurnSupport"
```

BurnSupport = off;

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

Fix Text: Configure the macOS system to disable writing to external optical media devices by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-257246

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257246r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005054](#)

Rule Title: The macOS system must be configured to disable prompts to configure Touch ID.

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

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

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

Check Content:

Verify the macOS system is configured to disable prompts to setup TouchID with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SkipTouchIDSetup"
```

SkipTouchIDSetup = 1;

If "SkipTouchIDSetup" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable prompts to setup TouchID by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257247

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257247r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-005055](#)

Rule Title: The macOS system must be configured to disable prompts to configure ScreenTime.

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

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

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

Check Content:

Verify the macOS system is configured to disable Screentime Setup with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SkipScreenTime"
```

```
SkipScreenTime = 1;
```

If "SkipScreenTime" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable Screentime Setup by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257248

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257248r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005056](#)

Rule Title: The macOS system must be configured to disable prompts to configure Unlock with Watch.

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

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

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

Check Content:

Verify the macOS system is configured to disable prompts to setup Unlock with Watch with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "SkipUnlockWithWatch"
```

SkipUnlockWithWatch = 1;

If "SkipUnlockWithWatch" is not set to "1", this is a finding.

Fix Text: Configure the macOS system to disable prompts to setup Unlock with Watch by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257249

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257249r958478_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-13-005058](#)

Rule Title: The macOS system must be configured to prevent activity continuation between Apple devices.

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

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

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

Check Content:

Verify the macOS system is configured to prevent activity continuation between Apple devices with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowActivityContinuation"
```

```
allowActivityContinuation = 0;
```

If "allowActivityContinuation" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to prevent activity continuation between Apple devices by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257250

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257250r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005060](#)

Rule Title: The macOS system must be configured to prevent password proximity sharing requests from nearby Apple devices.

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

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

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

Check Content:

Verify the macOS system is configured to prevent password proximity sharing with the following command:

```
/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowPasswordProximityRequests"
```

```
allowPasswordProximityRequests = 0;
```

If "allowPasswordProximityRequests" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to prevent password proximity sharing by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-257251

Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-257251r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-13-005061](#)

Rule Title: The macOS system must be configured to prevent users from erasing all system content and settings.

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

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

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

Check Content:

Verify the macOS system is configured to prevent users from erasing all system content and settings with the following command:

/usr/sbin/system_profiler SPConfigurationProfileDataType | /usr/bin/grep "allowEraseContentAndSettings"

allowEraseContentAndSettings = 0;

If "allowEraseContentAndSettings" is not set to "0", this is a finding.

Fix Text: Configure the macOS system to prevent users from erasing all system content and settings by installing the "Restrictions Policy" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-269981

Group Title: SRG-OS-000439-GPOS-00195

Rule ID: SV-269981r1038907_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-13-999999](#)

Rule Title: The macOS system must be a supported release.

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

Check Content:

Verify the operating system version.

Click the Apple icon on the menu at the top left corner of the screen and select the "About This Mac" option.

The name of the macOS release installed appears on the Overview tab in the resulting window. The precise version number installed is displayed below that.

If the installed version of macOS 13 is not supported, this is a finding.

Fix Text: Upgrade to a supported version of the operating system.

CCI: CCI-002605

UNCLASSIFIED