

UNCLASSIFIED



Apple macOS 14 (Sonoma) Security Technical Implementation Guide

Version: 2

Release: 3

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-259418

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

Rule ID: SV-259418r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000001](#)

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

Vulnerability Discussion: Disabling Apple watches is a necessary step to ensuring that the information system retains a session lock until the user reestablishes access using authorized identification and authentication procedures.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAutoUnlock').js
EOS
```

If the result is not "false", this is a finding.

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

CCI: CCI-000056

Group ID (Vulid): V-259419

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

Rule ID: SV-259419r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000002](#)

Rule Title: The macOS system must enforce screen saver password.

Vulnerability Discussion: Users must authenticate 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/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('askForPassword').js
EOS
```

If the result is not "true", 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 "com.apple.screensaver" configuration profile.

CCI: CCI-000056

Group ID (Vulid): V-259420

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

Rule ID: SV-259420r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000003](#)

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

Vulnerability Discussion: A screen saver must be enabled and the system must be configured to require a password to unlock once the screensaver has been on for a maximum of five seconds.

An unattended system with an excessive grace period is vulnerable to a malicious user.

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/bin/osascript -l JavaScript << EOS
function run() {
    let delay = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('askForPasswordDelay'))
    if ( delay <= 5 ) {
        return("true")
    } else {
        return("false")
    }
}
EOS
```

If the result is not "true", 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 "com.apple.screensaver" configuration profile.

CCI: CCI-000056

Group ID (Vulid): V-259421

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

Rule ID: SV-259421r1009577_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000005](#)

Rule Title: The macOS system must configure user session lock when a smart token is removed.

Vulnerability Discussion: The screen lock must be configured to initiate automatically when the smart token is removed from the system.

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the information system but do not want to log out because of the temporary nature of their absence. While a session lock is not an acceptable substitute for logging out of an information system for longer periods of time, they prevent a malicious user from accessing the information system when a user has removed their smart token.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')\  
.objectForKey('tokenRemovalAction').js  
EOS
```

If the result is not "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 "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

CCI: CCI-000057

CCI: CCI-000058

Group ID (Vulid): V-259422

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

Rule ID: SV-259422r958404_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000007](#)

Rule Title: The macOS system must disable hot corners.

Vulnerability Discussion: Hot corners must be disabled.

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Although hot corners can be used to initiate a session lock or to 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/bin/profiles -P -o stdout | /usr/bin/grep -Ec "'wvous-bl-corner' = 0|'wvous-br-corner' = 0|'wvous-tl-corner' = 0|'wvous-tr-corner' = 0'
```

If the result is not "4", this is a finding.

Fix Text: Configure the macOS system to disable hot corners by installing the "com.apple.ManagedClient.preferences" configuration profile.

CCI: CCI-000060

Group ID (Vulid): V-259423

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

Rule ID: SV-259423r958402_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000009](#)

Rule Title: The macOS system must prevent AdminHostInfo from being available at LoginWindow.

Vulnerability Discussion: The system must be configured to not display sensitive information at the LoginWindow. The key AdminHostInfo when configured will allow the HostName, IP Address, and operating system version and build to be displayed.

Check Content:

Verify the macOS system is configured to prevent AdminHostInfo from being available at LoginWindow with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectIsForcedForKey('AdminHostInfo')
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to prevent AdminHostInfo from being available at LoginWindow by installing the "com.apple.loginwindow" configuration profile.

CCI: CCI-000057

Group ID (Vulid): V-259424

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

Rule ID: SV-259424r958364_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000012](#)

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

Vulnerability Discussion: The macOS is able to be configured to set an automated termination for 72 hours or less for all temporary or emergency accounts upon account creation.

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 disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Although the ability to create and use emergency administrator accounts is necessary for performing system maintenance during emergencies, these accounts present vulnerabilities to the system if they are not disabled and removed when they are no longer needed. Configuring the macOS to automatically remove or disable emergency accounts within 72 hours of creation mitigates the risks posed if one were to be created and accidentally left active once the crisis is resolved.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon 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 can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

If temporary or emergency 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 or emergency accounts must be set to 72 hours (or less) when the temporary or emergency account

is created.

If no policy is enforced by a directory service, a password policy can be set with the "pwpolicy" utility. The variable names may vary depending on how the policy was set.

If there are no temporary or emergency accounts defined on the system, this is Not Applicable.

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

Check Content:

Verify if a password policy is enforced by a directory service by asking the system administrator (SA) or information system security officer (ISSO).

If no policy is enforced by a directory service, a password policy can be set with the "pwpolicy" utility. The variable names may vary depending on how the policy was set.

If there are no temporary or emergency accounts defined on the system, this is Not Applicable.

To check if the password policy is configured to disable a temporary or emergency account after 72 hours, run the following command to output the password policy to the screen, substituting the correct user name in place of username:

```
/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, there should be a <dict> section that 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 too great an amount of time to "policyAttributeCreationTime", this is a finding.

Fix Text: 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/pwpolicy -u username setaccountpolicies /path/to/file

CCI: CCI-000016

CCI: CCI-001682

Group ID (Vulid): V-259425

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

Rule ID: SV-259425r1038944_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000014](#)

Rule Title: The macOS system must enforce time synchronization.

Vulnerability Discussion: Time synchronization must be enforced on all networked systems.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

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

Check Content:

Verify the macOS system is configured to enforce time synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.timed')\
.objectForKey('TMAutomaticTimeOnlyEnabled').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enforce time synchronization by installing the "com.apple.timed" configuration profile.

CCI: CCI-004923

CCI: CCI-004926

CCI: CCI-004922

CCI: CCI-001891

CCI: CCI-002046

Group ID (Vulid): V-259428

Group Title: SRG-OS-000021-GPOS-00005

Rule ID: SV-259428r958388_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000022](#)

Rule Title: The macOS system must limit consecutive failed log on attempts to three.

Vulnerability Discussion: The macOS must be configured to limit the number of failed log on attempts to a maximum of three. When the maximum number of failed attempts is reached, the account must be locked for a period of time after.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

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

Check Content:

Verify the macOS system is configured to limit consecutive failed log on attempts to three with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath
'//dict/key[text()="policyAttributeMaximumFailedAuthentications"]/following-sibling::integer[1]/text()' - |
/usr/bin/awk '{ if ($1 <= 3) {print "yes"} else {print "no"} }'
```

If the result is not "yes", this is a finding.

Fix Text: Configure the macOS system to limit consecutive failed log on attempts to three by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile or by a directory service.

CCI: CCI-000044

CCI: CCI-002238

Group ID (Vulid): V-259429

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

Rule ID: SV-259429r958390_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000023](#)

Rule Title: The macOS system must display the Standard Mandatory DOD Notice and Consent Banner at remote log on.

Vulnerability Discussion: Displaying a standardized and approved use notification before granting access to the operating system ensures that users are provided with privacy and security notification verbiage that 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:

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

Verify 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

CCI: CCI-000050

Group ID (Vulid): V-259430

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

Rule ID: SV-259430r958390_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000024](#)

Rule Title: The macOS system must enforce SSH to display the Standard Mandatory DOD Notice and Consent Banner.

Vulnerability Discussion: Displaying a standardized and approved use notification before granting access to the

operating system ensures that users are provided with privacy and security notification verbiage that 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.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

Check Content:

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

```
/usr/sbin/sshd -G | /usr/bin/grep -c "^banner /etc/banner"
```

If the command does not return "1", this is a finding.

Fix Text: Configure the macOS system to display the contents of "/etc/banner" before granting access to the system by creating a plain text file in the /private/etc/ssh/sshd_config.d/ directory containing the following:

```
banner /etc/banner
```

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-259431

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

Rule ID: SV-259431r958390_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000025](#)

Rule Title: The macOS system must display the Standard Mandatory DOD Notice and Consent Banner at the login window.

Vulnerability Discussion: Displaying a standardized and approved use notification before granting access to the operating system ensures that users are provided with privacy and security notification verbiage that 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 policy banner will show if a "PolicyBanner.rtf" or "PolicyBanner.rtf.d" exists in the "/Library/Security" folder.

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 -ld /Library/Security/PolicyBanner.rtf* | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

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-259432

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

Rule ID: SV-259432r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000030](#)

Rule Title: The macOS system must configure audit log files to not contain access control lists.

Vulnerability Discussion: The audit log files must not contain access control lists (ACLs).

This rule ensures that audit information and audit files are configured to be readable and writable only by system administrators, thereby preventing unauthorized access, modification, and deletion of files.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -le $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $1}'  
| /usr/bin/grep -c ":",
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system without ACLs applied to log files with the following command:

```
/bin/chmod -RN /var/audit
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259433

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

Rule ID: SV-259433r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000031](#)

Rule Title: The macOS system must configure audit log folders to not contain access control lists.

Vulnerability Discussion: The audit log folder must not contain access control lists (ACLs).

Audit logs contain sensitive data about the system and users. This rule ensures that the audit service is configured to create log folders that are readable and writable only by system administrators in order to prevent normal users from reading audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -lde /var/audit | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":"
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system without ACLs applied to log folders with the following command:

```
/bin/chmod -N /var/audit
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259434

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259434r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000033](#)

Rule Title: The macOS system must disable FileVault automatic log on.

Vulnerability Discussion: If FileVault is enabled, automatic log on must be disabled, so that both FileVault and login window authentication are required.

The default behavior of macOS when FileVault is enabled is to automatically log on to the computer once successfully passing user's FileVault credentials.

Note: DisableFDEAutoLogin does not have to be set on Apple Silicon-based macOS systems that are smartcard enforced, as smartcards are available at preboot.

Check Content:

Verify the macOS system is configured to disable filevault automatic login with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('DisableFDEAutoLogin').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable filevault automatic login by installing the "com.apple.loginwindow" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

CCI: CCI-000213

Group ID (Vulid): V-259435

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

Rule ID: SV-259435r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000051](#)

Rule Title: The macOS system must configure SSHD ClientAliveInterval to 900.

Vulnerability Discussion: If SSHD is enabled, then it must be configured with the Client Alive Interval set to 900.

Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client.

This setting works in conjunction with ClientAliveCountMax to determine the termination of the connection after the threshold has been reached.

Note: This setting is not intended to manage idle user sessions where there is no input from the client. Its purpose is to monitor for interruptions in network connectivity and force the session to terminate after the connection appears to be broken.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Check Content:

Verify the macOS system is configured to set the SSHD ClientAliveInterval to 900 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/clientaliveinterval/{print $2}'
```

If the result is not "900", this is a finding.

Fix Text: Configure the macOS system to set the SSHD ClientAliveInterval to 900 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')

if [[ -z $include_dir ]]; then
```

```

/usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\*/" /etc/ssh/sshd_config
fi

/usr/bin/grep -qxF 'clientaliveinterval 900' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo
"clientaliveinterval 900" >> "${include_dir}01-mscp-sshd.conf"

for file in $(ls ${include_dir}); do
    if [[ "$file" == "100-macos.conf" ]]; then
        continue
    fi
    if [[ "$file" == "01-mscp-sshd.conf" ]]; then
        break
    fi
    /bin/mv ${include_dir}${file} ${include_dir}20-${file}
done

```

CCI: CCI-001133

Group ID (Vulid): V-259436

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

Rule ID: SV-259436r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000052](#)

Rule Title: The macOS system must configure SSHD ClientAliveCountMax to 1.

Vulnerability Discussion: If SSHD is enabled it must be configured with the Client Alive Maximum Count set to 1.

This will set the number of client alive messages which may be sent without the SSH server receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, the SSH server will disconnect the client, terminating the session. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive.

Note: This setting is not intended to manage idle user sessions where there is no input from the client. Its purpose is to monitor for interruptions in network connectivity and force the session to terminate after the connection appears to be broken.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Check Content:

Verify the macOS system is configured to set the SSHD ClientAliveCountMax to 1 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/clientalivecountmax/{print $2}'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to set the SSHD ClientAliveCountMax to 1 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')
```

```
if [[ -z $include_dir ]]; then
```

```
/usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\*/" /etc/ssh/sshd_config
fi
```

```
/usr/bin/grep -qxF 'clntalivecountmax 1' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo
"clntalivecountmax 1" >> "${include_dir}01-mscp-sshd.conf"
```

```
for file in $(ls ${include_dir}); do
  if [[ "$file" == "100-macos.conf" ]]; then
    continue
  fi
  if [[ "$file" == "01-mscp-sshd.conf" ]]; then
    break
  fi
  /bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-001133

Group ID (Vulid): V-259437

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

Rule ID: SV-259437r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000053](#)

Rule Title: The macOS system must set Login Grace Time to 30.

Vulnerability Discussion: If SSHD is enabled, then it must be configured to wait only 30 seconds before timing out logon attempts.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Check Content:

Verify the macOS system is configured to set Login Grace Time to 30 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/logingracetime/{print $2}'
```

If the result is not "30", this is a finding.

Fix Text: Configure the macOS system to set Login Grace Time to 30 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')
```

```
if [[ -z $include_dir ]]; then
  /usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\*/" /etc/ssh/sshd_config
fi
```

```
/usr/bin/grep -qxF 'logingracetime 30' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo "logingracetime
30" >> "${include_dir}01-mscp-sshd.conf"
```

```
for file in $(ls ${include_dir}); do
  if [[ "$file" == "100-macos.conf" ]]; then
    continue
  fi
```

```
if [[ "$file" == "01-mscp-sshd.conf" ]]; then
    break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-001133

Group ID (Vulid): V-259438

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

Rule ID: SV-259438r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-000054](#)

Rule Title: The macOS system must limit SSHD to FIPS-compliant connections.

Vulnerability Discussion: If SSHD is enabled then it must be configured to limit the Ciphers, HostbasedAcceptedAlgorithms, HostKeyAlgorithms, KexAlgorithms, MACs, PubkeyAcceptedAlgorithms, CASignatureAlgorithms to algorithms that are FIPS 140 validated.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meet federal requirements.

Operating systems utilizing encryption must use FIPS validated mechanisms for authenticating to cryptographic modules.

Note: For more information on FIPS compliance with the version of SSHD included in the macOS, the manual page `apple_ssh_and_fips` has additional information.

Satisfies: SRG-OS-000033-GPOS-00014,SRG-OS-000120-GPOS-00061,SRG-OS-000250-GPOS-00093,SRG-OS-000393-GPOS-00173,SRG-OS-000394-GPOS-00174,SRG-OS-000396-GPOS-00176,SRG-OS-000424-GPOS-00188,SRG-OS-000478-GPOS-00223

Check Content:

Verify the macOS system is configured to limit SSHD to FIPS-compliant connections with the following command:

```
fips_sshd_config=("Ciphers aes128-gcm@openssh.com" "HostbasedAcceptedAlgorithms ecdsa-sha2-
nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-
nistp256-cert-v01@openssh.com" "KexAlgorithms ecdh-sha2-nistp256" "MACs hmac-sha2-256"
"PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com"
"CASignatureAlgorithms ecdsa-sha2-nistp256")
total=0
for config in $fips_sshd_config; do
    total=$((expr $(/usr/sbin/sshd -G | /usr/bin/grep -i -c "$config") + $total))
done

echo $total
```

If the result is not "7", this is a finding.

Fix Text: Configure the macOS system to limit SSHD to FIPS-compliant connections with the following command:

```
fips_sshd_config="Ciphers aes128-gcm@openssh.com
HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
KexAlgorithms ecdh-sha2-nistp256
MACs hmac-sha2-256
PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
CASignatureAlgorithms ecdsa-sha2-nistp256"
/bin/echo "${fips_sshd_config}" > /etc/ssh/sshd_config.d/fips_sshd_config
```

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

CCI: CCI-002421

CCI: CCI-002450

CCI: CCI-002890

CCI: CCI-003123

Group ID (Vulid): V-259439

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

Rule ID: SV-259439r958408_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-000057](#)

Rule Title: The macOS system must limit SSH to FIPS-compliant connections.

Vulnerability Discussion: SSH must be configured to limit the Ciphers, HostbasedAcceptedAlgorithms, HostKeyAlgorithms, KexAlgorithms, MACs, PubkeyAcceptedAlgorithms, CASignatureAlgorithms to algorithms that are FIPS 140 validated.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meet federal requirements.

Operating systems utilizing encryption must use FIPS-validated mechanisms for authenticating to cryptographic modules.

Note: For more information on FIPS compliance with the version of SSH included in the macOS, the manual page `apple_ssh_and_fips` has additional information.

Satisfies: SRG-OS-000033-GPOS-00014,SRG-OS-000120-GPOS-00061,SRG-OS-000250-GPOS-00093,SRG-OS-000396-GPOS-00176,SRG-OS-000424-GPOS-00188,SRG-OS-000478-GPOS-00223

Check Content:

Verify the macOS system is configured to limit SSH to FIPS-compliant connections with the following

command:

```
fips_ssh_config="Host *
Ciphers aes128-gcm@openssh.com
HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
KexAlgorithms ecdh-sha2-nistp256
MACs hmac-sha2-256
PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
CASignatureAlgorithms ecdsa-sha2-nistp256"
/usr/bin/grep -c "$fips_ssh_config" /etc/ssh/ssh_config.d/fips_ssh_config
```

If the result is not "8", this is a finding.

Fix Text: Configure the macOS system to limit SSH to FIPS-compliant connections with the following command:

```
fips_ssh_config="Host *
Ciphers aes128-gcm@openssh.com
HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
KexAlgorithms ecdh-sha2-nistp256
MACs hmac-sha2-256
PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
CASignatureAlgorithms ecdsa-sha2-nistp256"
/bin/echo "${fips_ssh_config}" > /etc/ssh/ssh_config.d/fips_ssh_config
```

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

CCI: CCI-002421

CCI: CCI-002450

Group ID (Vulid): V-259440

Group Title: SRG-OS-000021-GPOS-00005

Rule ID: SV-259440r958388_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000060](#)

Rule Title: The macOS system must set account lockout time to 15 minutes.

Vulnerability Discussion: The macOS must be configured to enforce a lockout time period of at least 15 minutes when the maximum number of failed logon attempts is reached.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

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

Check Content:

Verify the macOS system is configured to set account lockout time to 15 minutes with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath
'//dict/key[text()="autoEnableInSeconds"]/following-sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1/60 >= 15 )
{print "yes"}} else {print "no"}}'
```

If the result is not "yes", this is a finding.

Fix Text: Configure the macOS system to set account lockout time to 15 minutes by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile or by a directory service.

CCI: CCI-000044

CCI: CCI-002238

Group ID (Vulid): V-259441

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

Rule ID: SV-259441r958402_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000070](#)

Rule Title: The macOS system must enforce screen saver timeout.

Vulnerability Discussion: The screen saver timeout must be set to 900 seconds or a shorter length of time.

This rule ensures that a full session lock is triggered within no more than 900 seconds of inactivity.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
    let timeout = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')\
.objectForKey('idleTime'))
    if ( timeout <= 900 ) {
        return("true")
    } else {
        return("false")
    }
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to initiate the screen saver after 15 minutes of inactivity by installing the "com.apple.screensaver" configuration profile.

CCI: CCI-000057

Group ID (Vulid): V-259443

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-259443r1009579_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000090](#)

Rule Title: The macOS system must disable logon to other user's active and locked sessions.

Vulnerability Discussion: The ability to log in to another user's active or locked session must be disabled.

macOS has a privilege that can be granted to any user that will allow that user to unlock active user's sessions. Disabling the admins and/or user's ability to log into another user's active and locked session prevents unauthorized persons from viewing potentially sensitive and/or personal information.

Note: Configuring this setting will disable TouchID from unlocking the screensaver.

Check Content:

Verify the macOS system is configured to disable login to other user's active and locked sessions with the following command:

```
/usr/bin/security authorizationdb read system.login.screensaver 2>&1 | /usr/bin/grep -c '<string>authenticate-session-owner</string>'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable login to other user's active and locked sessions with the following command:

```
/usr/bin/security authorizationdb write system.login.screensaver "authenticate-session-owner"
```

CCI: CCI-000764

CCI: CCI-004045

CCI: CCI-000770

Group ID (Vulid): V-259444

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-259444r1009580_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000100](#)

Rule Title: The macOS system must disable root logon.

Vulnerability Discussion: To ensure individual accountability and prevent unauthorized access, logging in as root at the login window must be disabled.

The macOS system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator, and administrator users must never log in directly as root.

Satisfies: SRG-OS-000104-GPOS-00051,SRG-OS-000109-GPOS-00056,SRG-OS-000364-GPOS-00151

Check Content:

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

```
/usr/bin/dscl . -read /Users/root UserShell 2>&1 | /usr/bin/grep -c "/usr/bin/false"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable root login with the following command:

```
/usr/bin/dscl . -create /Users/root UserShell /usr/bin/false
```

CCI: CCI-000764

CCI: CCI-004045

CCI: CCI-001813

CCI: CCI-000770

Group ID (Vulid): V-259445

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

Rule ID: SV-259445r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000110](#)

Rule Title: The macOS system must configure SSH ServerAliveInterval option set to 900.

Vulnerability Discussion: SSH must be configured with an Active Server Alive Maximum Count set to 900.

Setting the Active Server Alive Maximum Count to 900 will log users out after a 900-second interval of inactivity.

Note: /etc/ssh/ssh_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Check Content:

Verify the macOS system is configured to set the SSH ServerAliveInterval option set to 900 with the following command:

```
ret="pass"
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
  sshCheck=$(/usr/bin/sudo -u $u /usr/bin/ssh -G . | /usr/bin/grep -c "^serveraliveinterval 900")
  if [[ "$sshCheck" == "0" ]]; then
    ret="fail"
    break
  fi
done
/bin/echo $ret
```

If the result is not "pass", this is a finding.

Fix Text: Configure the macOS system to set the SSH ServerAliveInterval option set to 900 with the following command:

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
    config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1 | /usr/bin/awk '/Reading configuration data/ {print $NF}' |
/usr/bin/tr -d '\r')
    configarray=( ${f}config )
    for c in $configarray; do
        /usr/bin/sudo -u $u /usr/bin/grep -q '^ServerAliveInterval' "$c" && /usr/bin/sed -i "
's/. *ServerAliveInterval.*/ServerAliveInterval 900/' "$c" || /bin/echo 'ServerAliveInterval 900' >> "$c"
    done
done
```

CCI: CCI-001133

Group ID (Vulid): V-259446

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

Rule ID: SV-259446r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000120](#)

Rule Title: The macOS system must configure SSHD Channel Timeout to 900.

Vulnerability Discussion: If SSHD is enabled it must be configured with session Channel Timeout set to 900.

This will set the time out when the session is inactive.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

Check Content:

Verify the macOS system is configured to set the SSHD Channel Timeout to 900 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk -F "=" '/channeltimout session:*/{print $2}'
```

If the result is not "900", this is a finding.

Fix Text: Configure the macOS system to set the SSHD Channel Timeout to 900 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')
```

```
if [[ -z $include_dir ]]; then
```

```
    /usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\*/" /etc/ssh/sshd_config
```

```
fi
```

```
/usr/bin/grep -qxF 'channeltimout session:*=900' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo
"channeltimout session:*=900" >> "${include_dir}01-mscp-sshd.conf"
```

```
for file in $(ls ${include_dir}); do
```

```
    if [[ "$file" == "100-macos.conf" ]]; then
```

```
        continue
```

```
    fi
```

```
if [[ "$file" == "01-mscp-sshd.conf" ]]; then
    break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-001133

CCI: CCI-002361

Group ID (Vulid): V-259447

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

Rule ID: SV-259447r1009527_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000130](#)

Rule Title: The macOS system must configure SSHD unused connection timeout to 900.

Vulnerability Discussion: If SSHD is enabled, it must be configured with unused connection timeout set to 900.

This will set the timeout when there are no open channels within a session.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

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

Check Content:

Verify the macOS system is configured to set the SSHD unused connection timeout to 900 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/unusedconnectiontimeout/{print $2}'
```

If the result is not "900", this is a finding.

Fix Text: Configure the macOS system to set the SSHD unused connection timeout to 900 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')
```

```
if [[ -z $include_dir ]]; then
    /usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\\"*/" /etc/ssh/sshd_config
fi
```

```
/usr/bin/grep -qxF 'unusedconnectiontimeout 900' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo
"unusedconnectiontimeout 900" >> "${include_dir}01-mscp-sshd.conf"
```

```
for file in $(ls ${include_dir}); do
    if [[ "$file" == "100-macos.conf" ]]; then
        continue
    fi
    if [[ "$file" == "01-mscp-sshd.conf" ]]; then
        break
    fi
done
```

```
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-001133

CCI: CCI-002361

Group ID (Vulid): V-259448

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

Rule ID: SV-259448r970703_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000140](#)

Rule Title: The macOS system must set SSH Active Server Alive Maximum to 0.

Vulnerability Discussion: SSH must be configured with an Active Server Alive Maximum Count set to 0. Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session or an incomplete login attempt will also free up resources committed by the managed network element.

Note: /etc/ssh/ssh_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Check Content:

Verify the macOS system is configured to set SSH Active Server Alive Maximum to 0 with the following command:

```
ret="pass"
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
  sshCheck=$(/usr/bin/sudo -u $u /usr/bin/ssh -G . | /usr/bin/grep -c "^serveralivecountmax 0")
  if [[ "$sshCheck" == "0" ]]; then
    ret="fail"
    break
  fi
done
/bin/echo $ret
```

If the result is not "pass", this is a finding.

Fix Text: Configure the macOS system to set SSH Active Server Alive Maximum to 0 with the following command:

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
  config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1 | /usr/bin/awk '/Reading configuration data/ {print $NF}')
  /usr/bin/tr -d '\r')
  configarray=( ${f}config )
  for c in $configarray; do
    /usr/bin/sudo -u $u /usr/bin/grep -q '^ServerAliveCountMax' "$c" && /usr/bin/sed -i "
's/. *ServerAliveCountMax.*/ServerAliveCountMax 0/' "$c" || /bin/echo 'ServerAliveCountMax 0' >> "$c"
  done
done
```

Group ID (Vulid): V-259449

Group Title: SRG-OS-000279-GPOS-00109

Rule ID: SV-259449r958636_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000160](#)

Rule Title: The macOS system must enforce auto logout after 86400 seconds of inactivity.

Vulnerability Discussion: Auto logout must be configured to automatically terminate a user session and log out the after 86400 seconds of inactivity.

Note: The maximum that macOS can be configured for autologoff is 86400 seconds.

[IMPORTANT]

=====
The automatic logout may cause disruptions to an organization's workflow and/or loss of data. Information system security officers (ISSOs) are advised to first fully weigh the potential risks posed to their organization before opting to disable the automatic logout setting.
=====

Check Content:

Verify the macOS system is configured to enforce auto logout after 86400 seconds of inactivity with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('.GlobalPreferences')\
.objectForKey('com.apple.autologout.AutoLogOutDelay').js
EOS
```

If the result is not "86400", this is a finding.

Fix Text: Configure the macOS system to enforce auto logout after 86400 seconds of inactivity by installing the "com.apple.GlobalPreferences" configuration profile.

Group ID (Vulid): V-259450

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

Rule ID: SV-259450r1038944_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000170](#)

Rule Title: The macOS system must be configured to use an authorized time server.

Vulnerability Discussion: Approved time servers must be the only servers configured for use.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

An authoritative time server is synchronized with redundant United States Naval Observatory (USNO) time

servers as designated for the appropriate DOD network.

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

Check Content:

Verify the macOS system is configured to use an authorized time server with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('timeServer').js
EOS
```

If the result is not an authoritative time server which is synchronized with redundant USNO time servers as designated for the appropriate DOD network, this is a finding.

Fix Text: Configure the macOS system to use an authorized time server by installing the "com.apple.MCX" configuration profile.

CCI: CCI-004923

CCI: CCI-004926

CCI: CCI-001891

CCI: CCI-002046

Group ID (Vulid): V-259451

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

Rule ID: SV-259451r1038944_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-000180](#)

Rule Title: The macOS system must enable time synchronization daemon.

Vulnerability Discussion: The macOS time synchronization daemon (timed) must be enabled for proper time synchronization to an authorized time server.

Note: The time synchronization daemon is enabled by default on macOS.

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

Check Content:

Verify the macOS system is configured to enable time synchronization daemon with the following command:

```
/bin/launchctl list | /usr/bin/grep -c com.apple.timed
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to enable time synchronization daemon with the following command:

```
/bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.timed.plist
```

CCI: CCI-004923

CCI: CCI-004926

CCI: CCI-004922

CCI: CCI-001891

CCI: CCI-002046

Group ID (Vulid): V-259452

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

Rule ID: SV-259452r1009583_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001001](#)

Rule Title: The macOS system must be configured to audit all administrative action events.

Vulnerability Discussion: Administrative action events include changes made to the system (e.g., modifying authentication policies). If audit records do not include "ad" events, it is difficult to identify incidents and to correlate incidents to subsequent events. Audit records can be generated from various components within the information system (e.g., via a module or policy filter).

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.

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-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000476-GPOS-00221

Check Content:

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

```
/usr/bin/awk -F' ' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec 'ad'
```

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/grep -qE "^(^flags.*[^-]ad" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,ad/'  
/etc/security/audit_control; /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-003938

CCI: CCI-002234

CCI: CCI-002884

CCI: CCI-004188

CCI: CCI-001814

Group ID (Vulid): V-259453

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

Rule ID: SV-259453r958406_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001002](#)

Rule Title: The macOS system must be configured to audit all log on and log out events.

Vulnerability Discussion: The audit system must be configured to record all attempts to log in and out of the system (lo).

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 in order to proceed. Auditing both successful and unsuccessful attempts to switch to another user account (by way of monitoring log on and log out events) mitigates this risk.

The information system monitors log on and log out events.

Satisfies: SRG-OS-000032-GPOS-00013,SRG-OS-000064-GPOS-00033,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000470-GPOS-00214,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000472-GPOS-00217,SRG-OS-000473-GPOS-00218

Check Content:

Verify the macOS system is configured to audit all log on and log out events with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec '^lo'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to audit all log on and log out events with the following command:

```
/usr/bin/grep -qE "^flags.*[^\n]lo" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,lo/'  
/etc/security/audit_control; /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

CCI: CCI-002884

Group ID (Vulid): V-259454

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

Rule ID: SV-259454r1009584_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001003](#)

Rule Title: The macOS system must enable security auditing.

Vulnerability Discussion: Audit records establish what types of events have occurred, when they occurred, and which users were involved. These records aid an organization in their efforts to establish, correlate, and investigate the events leading up to an outage or attack.

The content required to be captured in an audit record varies based on the impact level of an organization's system. Content that may be necessary to satisfy this requirement includes, for example, time stamps, source addresses, destination addresses, user identifiers, event descriptions, success/fail indications, filenames involved, and access or flow control rules invoked.

The information system initiates session audits at system startup.

Note: Security auditing is enabled by default on macOS.

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-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000303-GPOS-00120,SRG-OS-000337-GPOS-00129,SRG-OS-000358-GPOS-00145,SRG-OS-000359-GPOS-00146,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000461-GPOS-00205,SRG-OS-000462-GPOS-00206,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-000470-GPOS-00214,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000472-GPOS-00217,SRG-OS-000473-GPOS-00218,SRG-OS-000474-GPOS-00219,SRG-OS-000475-GPOS-00220,SRG-OS-000476-GPOS-00221,SRG-OS-000477-GPOS-00222

Check Content:

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

```
LAUNCHD_RUNNING=$(/bin/launchctl list | /usr/bin/grep -c com.apple.auditd)
if [[ $LAUNCHD_RUNNING == 1 ]] && [[ -e /etc/security/audit_control ]]; then
    echo "pass"
else
    echo "fail"
fi
```

If the result is not "pass", this is a finding.

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

```
LAUNCHD_RUNNING=$(/bin/launchctl list | /usr/bin/grep -c com.apple.auditd)
```

```
if [[ ! $LAUNCHD_RUNNING == 1 ]]; then
```

```
  /bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist
```

```
fi
```

```
if [[ ! -e /etc/security/audit_control ]] && [[ -e /etc/security/audit_control.example ]];then
```

```
  /bin/cp /etc/security/audit_control.example /etc/security/audit_control
```

```
else
```

```
  /usr/bin/touch /etc/security/audit_control
```

```
fi
```

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000159

CCI: CCI-000172

CCI: CCI-001464

CCI: CCI-001487

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-003938

CCI: CCI-001889

CCI: CCI-001890

CCI: CCI-001914

CCI: CCI-002130

CCI: CCI-002884

CCI: CCI-004188

CCI: CCI-001814

Group ID (Vulid): V-259455

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

Rule ID: SV-259455r1038966_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001010](#)

Rule Title: The macOS system must configure system to shut down upon audit failure.

Vulnerability Discussion: The audit service must be configured to 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 can occur due to software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

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/awk -F':' '/^policy/ {print $NF}' /etc/security/audit_control | /usr/bin/tr ',' '\n' | /usr/bin/grep -Ec 'ahlt'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to shut down upon audit failure with the following command:

```
/usr/bin/sed -i.bak 's/^policy.*/policy: ahl,argv/' /etc/security/audit_control; /usr/sbin/audit -s
```

CCI: CCI-000140

Group ID (Vulid): V-259456
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-259456r958434_rule
Severity: CAT II
Rule Version (STIG-ID): [APPL-14-001012](#)
Rule Title: The macOS system must configure audit log files to be owned by root.

Vulnerability Discussion: Audit log files must be owned by root.

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 system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$3}  
END {print s}'
```

If the result is not "0", this is a finding.

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

```
/usr/sbin/chown -R root /var/audit/*
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259457
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-259457r958434_rule
Severity: CAT II
Rule Version (STIG-ID): [APPL-14-001013](#)
Rule Title: The macOS system must configure audit log folders to be owned by root.

Vulnerability Discussion: Audit log folders must be owned by root.

The audit service must be configured to create log folders with the correct ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log folders are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -dn $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $3}'
```

If the result is not "0", this is a finding.

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

```
/usr/sbin/chown root /var/audit
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259458

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

Rule ID: SV-259458r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001014](#)

Rule Title: The macOS system must configure audit log files group to wheel.

Vulnerability Discussion: Audit log files must have the group set to wheel.

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 system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{s+=$4} END {print s}'
```

If the result is not "0", this is a finding.

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

```
/usr/bin/chgrp -R wheel /var/audit/*
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259459

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

Rule ID: SV-259459r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001015](#)

Rule Title: The macOS system must configure audit log folders group to wheel.

Vulnerability Discussion: Audit log folders must have the group set to wheel.

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 system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -dn $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $4}'
```

If the result is not "0", this is a finding.

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

```
/usr/bin/chgrp wheel /var/audit
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259460

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

Rule ID: SV-259460r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001016](#)

Rule Title: The macOS system must configure audit log files to mode 440 or less permissive.

Vulnerability Discussion: The audit service must be configured to create log files that are readable only by the root user and group wheel. To achieve this, audit log files must be configured to mode 440 or less permissive; thereby preventing normal users from reading, modifying, or deleting audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -l $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '!/-r--r-----|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

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

```
/bin/chmod 440 /var/audit/*
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259461

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

Rule ID: SV-259461r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001017](#)

Rule Title: The macOS system must configure audit log folders to mode 700 or less permissive.

Vulnerability Discussion: The audit log folder must be configured to mode 700 or less permissive so that only the root user is able to read, write, and execute changes to folders.

Because audit logs contain sensitive data about the system and users, the audit service must be configured to mode 700 or less permissive; thereby preventing normal users from reading, modifying, or deleting audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/usr/bin/stat -f %A $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

If the result is not a mode of 700 or less permissive, this is a finding.

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

```
/bin/chmod 700 /var/audit
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259462

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

Rule ID: SV-259462r1009585_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001020](#)

Rule Title: The macOS system must be configured to audit all deletions of object attributes.

Vulnerability Discussion: The audit system must be configured to record enforcement actions of attempts to delete file attributes (fd).

***Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. One common and effective enforcement action method is using access restrictions (i.e., denying modifications to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to delete a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000064-GPOS-00033,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,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

Check Content:

Verify the macOS system is configured to audit all deletions of object attributes with the following command:

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ',' '\n' | /usr/bin/grep -Ec '\-fd'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to audit all deletions of object attributes with the following command:

```
/usr/bin/grep -qE "^flags.*-fd" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/, -fd' /etc/security/audit_control;/usr/sbin/audit -s
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000172

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-003938

CCI: CCI-002884

CCI: CCI-001814

Group ID (Vulid): V-259463

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

Rule ID: SV-259463r1009586_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001021](#)

Rule Title: The macOS system must be configured to audit all changes of object attributes.

Vulnerability Discussion: The audit system must be configured to record enforcement actions of attempts to modify file attributes (fm).

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. One common and effective enforcement action method is using access restrictions (i.e., modifications to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions attempts to modify a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000064-GPOS-00033,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000462-GPOS-00206,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

Check Content:

Verify the macOS system is configured to audit all changes of object attributes with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF } /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec '^fm'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to audit all changes of object attributes with the following command:

```
/usr/bin/grep -qE "^flags.*fm" /etc/security/audit_control || /usr/bin/sed -i.bak 's/^flags/ s/$,fm/'  
/etc/security/audit_control;/usr/sbin/audit -s
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000172

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-003938

CCI: CCI-002884

CCI: CCI-001814

Group ID (Vulid): V-259464

Group Title: SRG-OS-000463-GPOS-00207

Rule ID: SV-259464r991573_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001022](#)

Rule Title: The macOS system must be configured to audit all failed read actions on the system.

Vulnerability Discussion: The audit system must be configured to record enforcement actions of access restrictions, including failed file read (-fr) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using access restrictions (e.g., denying access to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to read a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000463-GPOS-00207,SRG-OS-000057-GPOS-00027,SRG-OS-000465-GPOS-00209,SRG-OS-000474-GPOS-00219

Check Content:

Verify the macOS system is configured to audit all failed read actions on the system with the following

command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec '\-fr'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to audit all failed read actions on the system with the following command:

```
/usr/bin/grep -qE "^flags.*-fr" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/, -fr' /etc/security/audit_control;/usr/sbin/audit -s
```

CCI: CCI-000162

CCI: CCI-000172

Group ID (Vulid): V-259465

Group Title: SRG-OS-000463-GPOS-00207

Rule ID: SV-259465r991573_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001023](#)

Rule Title: The macOS system must be configured to audit all failed write actions on the system.

Vulnerability Discussion: The audit system must be configured to record enforcement actions of access restrictions, including failed file write (-fw) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using access restrictions (e.g., denying users access to edit a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to change a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000463-GPOS-00207,SRG-OS-000057-GPOS-00027,SRG-OS-000465-GPOS-00209,SRG-OS-000466-GPOS-00210,SRG-OS-000467-GPOS-00211,SRG-OS-000468-GPOS-00212

Check Content:

Verify the macOS system is configured to audit all failed write actions on the system with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec '\-fw'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to audit all failed write actions on the system with the following command:

```
/usr/bin/grep -qE "^flags.*-fw" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/, -fw' /etc/security/audit_control;/usr/sbin/audit -s
```

CCI: CCI-000162

CCI: CCI-000172

Group ID (Vulid): V-259466

Group Title: SRG-OS-000463-GPOS-00207

Rule ID: SV-259466r1009587_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001024](#)

Rule Title: The macOS system must be configured to audit all failed program execution on the system.

Vulnerability Discussion: The audit system must be configured to record enforcement actions of access restrictions, including failed program execute (-ex) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using program execution restrictions (e.g., denying users access to execute certain processes).

This configuration ensures that audit lists include events in which program execution has failed.

Without auditing the enforcement of program execution, it is difficult to identify attempted attacks as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000463-GPOS-00207,SRG-OS-000365-GPOS-00152,SRG-OS-000458-GPOS-00203,SRG-OS-000465-GPOS-00209

Check Content:

Verify the macOS system is configured to audit all failed program execution on the system with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ', ' '\n' | /usr/bin/grep -Ec '\-ex'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to audit all failed program execution on the system with the following command:

```
/usr/bin/grep -qE "^flags.*-ex" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/, -ex/'  
/etc/security/audit_control; /usr/sbin/audit -s
```

CCI: CCI-000172

CCI: CCI-003938

CCI: CCI-001814

Group ID (Vulid): V-259467

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

Rule ID: SV-259467r958752_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-14-001029](#)

Rule Title: The macOS system must configure audit retention to seven days.

Vulnerability Discussion: The audit service must be configured to require records be kept for an organizational defined value before deletion, unless the system uses a central audit record storage facility.

When "expire-after" is set to "7d", the audit service will not delete audit logs until the log data criteria is met.

Check Content:

Verify the macOS system is configured audit retention to seven days with the following command:

```
/usr/bin/awk -F: '/expire-after/{print $2}' /etc/security/audit_control
```

If the result is not "7d", this is a finding.

Fix Text: Configure the macOS system to set audit retention to seven days with the following command:

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

CCI: CCI-001849

Group ID (Vulid): V-259468

Group Title: SRG-OS-000046-GPOS-00022

Rule ID: SV-259468r958424_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001030](#)

Rule Title: The macOS system must configure audit capacity warning.

Vulnerability Discussion: The audit service must be configured to notify the system administrator when the amount of free disk space remaining reaches an organization defined value.

This rule ensures that the system administrator is notified in advance that action is required to free up more disk space for audit logs.

Satisfies: SRG-OS-000046-GPOS-00022,SRG-OS-000343-GPOS-00134

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/awk -F: '/^minfree/{print $2}' /etc/security/audit_control
```

If the result is not "25", this is a finding.

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

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

CCI: CCI-000139

Group ID (Vulid): V-259469

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

Rule ID: SV-259469r1038966_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001031](#)

Rule Title: The macOS system must configure audit failure notification.

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 made aware immediately 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 a potentially harmful failure in the auditing system's capability, and system operation may be adversely affected.

Satisfies: SRG-OS-000047-GPOS-00023,SRG-OS-000344-GPOS-00135

Check Content:

Verify the macOS system is configured to produce audit failure notification with the following command:

```
/usr/bin/grep -c "logger -s -p" /etc/security/audit_warn
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to produce audit failure notification with the following command:

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

CCI: CCI-000140

CCI: CCI-001858

Group ID (Vulid): V-259470

Group Title: SRG-OS-000365-GPOS-00152

Rule ID: SV-259470r1009588_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001044](#)

Rule Title: The macOS system must configure the system to audit all authorization and authentication events.

Vulnerability Discussion: The auditing system must be configured to flag authorization and authentication (aa) events.

Authentication events contain information about the identity of a user, server, or client. Authorization events contain information about permissions, rights, and rules. If audit records do not include aa events, it is difficult to identify incidents and to correlate incidents to subsequent events.

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

Satisfies: SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,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-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000475-GPOS-00220,SRG-OS-000477-GPOS-00222

Check Content:

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

```
/usr/bin/awk -F' ' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ', ' '\n' | /usr/bin/grep -Ec 'aa'
```

If the result is not "1", this is a finding.

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

```
/usr/bin/grep -qE "^flags.*[^-]aa" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,aa/'  
/etc/security/audit_control; /usr/sbin/audit -s
```

CCI: CCI-000172

CCI: CCI-003938

CCI: CCI-002884

CCI: CCI-001814

Group ID (Vulid): V-259471

Group Title: SRG-OS-000066-GPOS-00034

Rule ID: SV-259471r1009589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001060](#)

Rule Title: The macOS system must set smart card certificate trust to moderate.

Vulnerability Discussion: The macOS system must be configured to block access to users who are no longer authorized (i.e., users with revoked certificates).

To prevent the use of untrusted certificates, the certificates on a smart card must meet the following criteria: its issuer has a system-trusted certificate, the certificate is not expired, its "valid-after" date is in the past, and it passes Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) checking.

By setting the smart card certificate trust level to moderate, the system will execute a soft revocation, i.e., if the OCSP/CRL server is unreachable, authentication will still succeed.

Note: Before applying this setting, refer to the smart card supplemental guidance.

Satisfies: SRG-OS-000066-GPOS-00034,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/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')\
.objectForKey('checkCertificateTrust').js
EOS
```

If the result is not "2", this is a finding.

Fix Text: Configure the macOS system to check the revocation status of user certificates by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

CCI: CCI-000185

CCI: CCI-001954

CCI: CCI-004068

CCI: CCI-002470

CCI: CCI-001991

Group ID (Vulid): V-259472

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

Rule ID: SV-259472r1009590_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001100](#)

Rule Title: The macOS system must disable root logon for SSH.

Vulnerability Discussion: If SSH is enabled to ensure individual accountability and prevent unauthorized access, logging in as root via SSH must be disabled.

The macOS system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator, and administrator users must never log in directly as root.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000109-GPOS-00056,SRG-OS-000364-GPOS-00151

Check Content:

Verify the macOS system is configured to disable root login for SSH with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/permitrootlogin/{print $2}'
```

If the result is not "no", this is a finding.

Fix Text: Configure the macOS system to disable root login for SSH with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')

if [[ -z $include_dir ]]; then
  /usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\*/" /etc/ssh/sshd_config
fi

/usr/bin/grep -qxF 'permitrootlogin no' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo "permitrootlogin
no" >> "${include_dir}01-mscp-sshd.conf"

for file in $(ls ${include_dir}); do
  if [[ "$file" == "100-macos.conf" ]]; then
    continue
  fi
  if [[ "$file" == "01-mscp-sshd.conf" ]]; then
    break
  fi
  /bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-004045

CCI: CCI-001813

CCI: CCI-000770

Group ID (Vulid): V-259473

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

Rule ID: SV-259473r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001110](#)

Rule Title: The macOS system must configure audit_control group to wheel.

Vulnerability Discussion: /etc/security/audit_control must have the group set to wheel.

The audit service must be configured with the correct group ownership to prevent normal users from manipulation audit log configurations.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

Verify the macOS system is configured with the audit_control group to wheel with the following command:

```
/bin/ls -dn /etc/security/audit_control | /usr/bin/awk '{print $4}'
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system with the audit_control group to wheel with the following command:

```
/usr/bin/chgrp wheel /etc/security/audit_control
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000171

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259474

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

Rule ID: SV-259474r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001120](#)

Rule Title: The macOS system must configure audit_control owner to root.

Vulnerability Discussion: /etc/security/audit_control must have the owner set to root.

The audit service must be configured with the correct ownership to prevent normal users from manipulation audit log configurations.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

Verify the macOS system is configured with the audit_control owner to root with the following command:

```
/bin/ls -dn /etc/security/audit_control | /usr/bin/awk '{print $3}'
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system with the audit_control owner to root with the following command:

```
/usr/sbin/chown root /etc/security/audit_control
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000171

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259475

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

Rule ID: SV-259475r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001130](#)

Rule Title: The macOS system must configure audit_control to mode 440 or less permissive.

Vulnerability Discussion: /etc/security/audit_control must be configured so that it is readable only by the root user and group wheel.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

Verify the macOS system is configured audit_control to mode 440 or less with the following command:

```
/bin/ls -l /etc/security/audit_control | /usr/bin/awk '!/-r--[r-]-----|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/xargs
```

If the results are not "0", this is a finding.

Fix Text: Configure the macOS system with the audit_control to mode 440 with the following command:

```
/bin/chmod 440 /etc/security/audit_control
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000171

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

Group ID (Vulid): V-259476

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

Rule ID: SV-259476r958434_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-001140](#)

Rule Title: The macOS system must configure audit_control to not contain access control lists.

Vulnerability Discussion: /etc/security/audit_control must not contain Access Control Lists (ACLs).

/etc/security/audit_control contains sensitive configuration data about the audit service. This rule ensures that the audit service is configured to be readable and writable only by system administrators in order to prevent normal users from manipulating audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

Check Content:

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

```
/bin/ls -le /etc/security/audit_control | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":"
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system without ACLs applied to audit_control with the following command:

```
/bin/chmod -N /etc/security/audit_control
```

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000171

CCI: CCI-001493

CCI: CCI-001494

Group ID (Vulid): V-259477

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

Rule ID: SV-259477r1009591_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-001150](#)

Rule Title: The macOS system must disable password authentication for SSH.

Vulnerability Discussion: If remote logon through SSH is enabled, password-based authentication must be disabled for user logon.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

Note: /etc/ssh/sshd_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000067-GPOS-00035,SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057,SRG-OS-000125-GPOS-00065,SRG-OS-000375-GPOS-00160

Check Content:

Verify the macOS system is configured to disable password authentication for SSH with the following command:

```
/usr/sbin/sshd -G | /usr/bin/grep -Ec '^(passwordauthentication\s+no|kbdinteractiveauthentication\s+no)'
```

If the result is not "2", this is a finding.

Fix Text: Configure the macOS system to disable password authentication for SSH with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '*')
if [[ -z $include_dir ]]; then
  /usr/bin/sed -i.bk "1s/.*/Include \etc\ssh\sshd_config.d\*/" /etc/ssh/sshd_config
fi
echo "passwordauthentication no" >> "${include_dir}01-mscp-sshd.conf"
echo "kbdinteractiveauthentication no" >> "${include_dir}01-mscp-sshd.conf"

for file in $(ls ${include_dir}); do
  if [[ "$file" == "100-macos.conf" ]]; then
    continue
  fi
  if [[ "$file" == "01-mscp-sshd.conf" ]]; then
    break
  fi
  /bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-000186

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-000877

CCI: CCI-001941

CCI: CCI-004046

CCI: CCI-000767

CCI: CCI-000768

CCI: CCI-001948

Group ID (Vulid): V-259478

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259478r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002001](#)

Rule Title: The macOS system must disable Server Message Block sharing.

Vulnerability Discussion: Support for Server Message Block (SMB) file sharing is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities.

Check Content:

Verify the macOS system is configured to disable Server Message Block sharing with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.smbd" => disabled'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable Server Message Block sharing with the following command:

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

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

CCI: CCI-000213

Group ID (Vulid): V-259479

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259479r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002003](#)

Rule Title: The macOS system must disable Network File System service.

Vulnerability Discussion: Support for Network File Systems (NFS) services is nonessential and, therefore, must be disabled.

Check Content:

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

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.nfsd" => disabled'
```

If the result is not "1", this is a finding.

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

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

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

CCI: CCI-000213

Group ID (Vulid): V-259480

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

Rule ID: SV-259480r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002004](#)

Rule Title: The macOS system must disable Location Services.

Vulnerability Discussion: The information system must be configured to provide only essential capabilities. Disabling Location Services helps prevent the unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

Check Content:

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

```
/usr/bin/sudo -u _locationd /usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.locationd')\
.objectForKey('LocationServicesEnabled').js
EOS
```

If the result is not "false", this is a finding.

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

```
/usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd
LocationServicesEnabled -bool false; /bin/launchctl kickstart -k system/com.apple.locationd
```

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

CCI: CCI-000381

Group ID (Vulid): V-259481

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

Rule ID: SV-259481r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002005](#)

Rule Title: The macOS system must disable Bonjour multicast.

Vulnerability Discussion: Bonjour multicast advertising must be disabled to prevent the system from broadcasting its presence and available services over network interfaces.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mDNSResponder')\
.objectForKey('NoMulticastAdvertisements').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Bonjour multicast by installing the "com.apple.mDNSResponder" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259482

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259482r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002006](#)

Rule Title: The macOS system must disable Unix-to-Unix Copy Protocol service.

Vulnerability Discussion: The system must not have the Unix-to-Unix Copy Protocol (UUCP) service active.

UUCP, a set of programs that enable the sending of files between different Unix systems as well as sending commands to be executed on another system, is not essential and must be disabled in order to prevent the unauthorized connection of devices, transfer of information, and tunneling.

Note: UUCP service is disabled at startup by default macOS.

Check Content:

Verify the macOS system is configured to disable Unix-to-Unix copy protocol service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.uucp" => disabled'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable Unix-to-Unix copy protocol service with the following command:

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

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

CCI: CCI-000213

Group ID (Vulid): V-259483

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

Rule ID: SV-259483r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002007](#)

Rule Title: The macOS system must disable Internet Sharing.

Vulnerability Discussion: If the system does not require Internet Sharing, support for it is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling Internet sharing helps prevent the unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('forceInternetSharingOff').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Internet Sharing by installing the "com.apple.MCX" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259484

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259484r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002008](#)

Rule Title: The macOS system must disable the built-in web server.

Vulnerability Discussion: The built-in web server is a nonessential service built into macOS and must be disabled.

Note: The built in web server service is disabled at startup by default macOS.

Check Content:

Verify the macOS system is configured to disable the built-in web server with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "org.apache.httpd" => disabled'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable the built-in web server with the following command:

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

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

CCI: CCI-000213

Group ID (Vulid): V-259485

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259485r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002009](#)

Rule Title: The macOS system must disable AirDrop.

Vulnerability Discussion: AirDrop must be disabled to prevent file transfers to or from unauthorized devices. AirDrop allows users to share and receive files from other nearby Apple devices.

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000095-GPOS-00049,SRG-OS-000300-GPOS-00118

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirDrop').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable AirDrop by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000213

CCI: CCI-000381

CCI: CCI-001443

Group ID (Vulid): V-259486

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

Rule ID: SV-259486r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002010](#)

Rule Title: The macOS system must disable FaceTime.app.

Vulnerability Discussion: The macOS built-in FaceTime.app must be disabled.

The FaceTime.app establishes a connection to Apple's iCloud service, even when security controls have been put

in place to disable iCloud access.

[IMPORTANT]

Apple has deprecated the use of application restriction controls (<https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.new.L70>). Using these controls may not work as expected. Third-party software may be required to fulfill the compliance requirements.

Check Content:

Verify the macOS system is configured to disable FaceTime.app with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')\
  .objectForKey('familyControlsEnabled'))
  let pathlist = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')\
  .objectForKey('pathBlackList').js
  for ( let app in pathlist ) {
    if ( ObjC.unwrap(pathlist[app]) == "/Applications/FaceTime.app" && pref1 == true ){
      return("true")
    }
  }
  return("false")
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable FaceTime.app by installing the "com.apple.applicationaccess.new" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259487

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

Rule ID: SV-259487r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002012](#)

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

Vulnerability Discussion: The macOS built-in Calendar.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated calendar synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\  
.objectForKey('allowCloudCalendar').js  
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Calendar services by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259488

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

Rule ID: SV-259488r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002013](#)

Rule Title: The macOS system must disable iCloud Reminders.

Vulnerability Discussion: The macOS built-in Reminders.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated reminders synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\  
.objectForKey('allowCloudReminders').js  
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Reminders by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259489

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

Rule ID: SV-259489r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002014](#)

Rule Title: The macOS system must disable iCloud Address Book.

Vulnerability Discussion: The macOS built-in Contacts.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data, and, therefore, automated contact synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudAddressBook').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Address Book by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259490

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

Rule ID: SV-259490r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002015](#)

Rule Title: The macOS system must disable iCloud Mail.

Vulnerability Discussion: The macOS built-in Mail.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated mail synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudMail').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Mail by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259491

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

Rule ID: SV-259491r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002016](#)

Rule Title: The macOS system must disable iCloud Notes.

Vulnerability Discussion: The macOS built-in Notes.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated Notes synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudNotes').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Notes by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259492

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

Rule ID: SV-259492r1009529_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002017](#)

Rule Title: The macOS system must disable the camera.

Vulnerability Discussion: macOS must be configured to disable the camera.

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 authorizing official (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, verify the macOS system is configured to disable the camera with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCamera').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable the camera by installing the "com.apple.applicationaccess"

configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259493

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

Rule ID: SV-259493r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002020](#)

Rule Title: The macOS system must disable Siri.

Vulnerability Discussion: Support for Siri is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAssistant').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable Siri by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259494

Group Title: SRG-OS-000205-GPOS-00083

Rule ID: SV-259494r958564_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002021](#)

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

Vulnerability Discussion: The ability to submit diagnostic data to Apple must be disabled.

The information system must be configured to provide only essential capabilities. Disabling the submission of diagnostic and usage information will mitigate the risk of unwanted data being sent to Apple.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.SubmitDiagInfo')\
```

```
.objectForKey('AutoSubmit').js
let pref2 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowDiagnosticSubmission').js
if ( pref1 == false && pref2 == false ){
    return("true")
} else {
    return("false")
}
}
}
EOS
```

If the result is not "true", this is a finding.

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

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-259495

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259495r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002022](#)

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

Vulnerability Discussion: If the system does not require Remote Apple Events, support for Apple Remote Events is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling Remote Apple Events helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000096-GPOS-00050

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 -c "com.apple.AEServer" => disabled'
```

If the result is not "1", this is a finding.

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

```
/usr/sbin/systemsetup -setremoteappleevents off
/bin/launchctl disable system/com.apple.AEServer
```

Note: Systemsetup with -setremoteappleevents flag will fail unless Full Disk Access to systemsetup or its parent process is granted. This requires supervision.

CCI: CCI-000213

Group ID (Vulid): V-259496

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

Rule ID: SV-259496r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002035](#)

Rule Title: The macOS system must disable Apple ID setup during Setup Assistant.

Vulnerability Discussion: The prompt for Apple ID setup during Setup Assistant must be disabled.

macOS will automatically prompt new users to set up an Apple ID while they are going through Setup Assistant if this is not disabled, misleading new users to think they need to create Apple ID accounts upon their first log on.

Check Content:

Verify the macOS system is configured to disable Apple ID setup during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipCloudSetup').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Apple ID setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Group ID (Vulid): V-259497

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

Rule ID: SV-259497r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002036](#)

Rule Title: The macOS system must disable Privacy Setup services during Setup Assistant.

Vulnerability Discussion: The prompt for Privacy Setup services during Setup Assistant must be disabled.

Organizations must apply organizationwide configuration settings. The macOS Privacy Setup services prompt guides new users through enabling their own specific privacy settings; this is not essential and, therefore, must be disabled to prevent against the risk of individuals electing privacy settings with the potential to override organizationwide settings.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
```

```
.objectForKey('SkipPrivacySetup').js  
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Privacy Setup services during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259498

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

Rule ID: SV-259498r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002037](#)

Rule Title: The macOS system must disable iCloud Storage Setup during Setup Assistant.

Vulnerability Discussion: The prompt to set up iCloud storage services during Setup Assistant must be disabled.

The default behavior of macOS is to prompt new users to set up storage in iCloud. Disabling the iCloud storage setup prompt provides organizations more control over the storage of their data.

Check Content:

Verify the macOS system is configured to disable iCloud Storage Setup during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\  
.objectForKey('SkipiCloudStorageSetup').js  
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Storage Setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259499

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

Rule ID: SV-259499r987796_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-002038](#)

Rule Title: The macOS system must disable Trivial File Transfer Protocol service.

Vulnerability Discussion: If the system does not require Trivial File Transfer Protocol (TFTP), support it is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling TFTP helps prevent the unauthorized connection of devices and the unauthorized transfer of information.

Note: TFTP service is disabled at startup by default macOS.

Satisfies: SRG-OS-000074-GPOS-00042,SRG-OS-000080-GPOS-00048

Check Content:

Verify the macOS system is configured to disable trivial file transfer protocol service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.tftpd" => disabled'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable trivial file transfer protocol service with the following command:

```
/bin/launchctl disable system/com.apple.tftpd
```

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

CCI: CCI-000197

CCI: CCI-000213

Group ID (Vulid): V-259500

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

Rule ID: SV-259500r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002039](#)

Rule Title: The macOS system must disable Siri Setup during Setup Assistant.

Vulnerability Discussion: The prompt for Siri during Setup Assistant must be disabled.

Organizations must apply organizationwide configuration settings. The macOS Siri Assistant Setup prompt guides new users through enabling their own specific Siri settings; this is not essential and, therefore, must be disabled to prevent against the risk of individuals electing Siri settings with the potential to override organizationwide settings.

Check Content:

Verify the macOS system is configured to disable Siri Setup during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipSiriSetup').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Siri Setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259501
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-259501r958478_rule
Severity: CAT II
Rule Version (STIG-ID): [APPL-14-002040](#)
Rule Title: The macOS system must disable iCloud Keychain synchronization.

Vulnerability Discussion: The macOS system's ability to automatically synchronize a user's passwords to their iCloud account must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, password management and synchronization must be controlled by an organization approved service.

Check Content:

Verify the macOS system is configured to disable iCloud Keychain synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudKeychainSync').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Keychain synchronization by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259502
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-259502r958478_rule
Severity: CAT II
Rule Version (STIG-ID): [APPL-14-002041](#)
Rule Title: The macOS system must disable iCloud Document synchronization.

Vulnerability Discussion: The macOS built-in iCloud document synchronization service must be disabled to prevent organizational data from being synchronized to personal or nonapproved storage.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated document synchronization must be controlled by an organization approved service.

Check Content:

Verify the macOS system is configured to disable iCloud Document synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudDocumentSync').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Document synchronization by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259503

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

Rule ID: SV-259503r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002042](#)

Rule Title: The macOS system must disable iCloud Bookmarks.

Vulnerability Discussion: The macOS built-in Safari.app bookmark synchronization via the iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated bookmark synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudBookmarks').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Bookmarks by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259504

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

Rule ID: SV-259504r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002043](#)

Rule Title: The macOS system must disable iCloud Photo Library.

Vulnerability Discussion: The macOS built-in Photos.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated photo synchronization must be controlled by an organization approved service.

Check Content:

Verify the macOS system is configured to disable the iCloud Photo Library with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\  
.objectForKey('allowCloudPhotoLibrary').js  
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable the iCloud Photo Library by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259505

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259505r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002050](#)

Rule Title: The macOS system must disable Screen Sharing and Apple Remote Desktop.

Vulnerability Discussion: Support for both Screen Sharing and Apple Remote Desktop (ARD) is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling screen sharing and ARD helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

Check Content:

Verify the macOS system is configured to disable Screen Sharing and Apple Remote Desktop with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.screensharing" => disabled'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable Screen Sharing and Apple Remote Desktop with the following command:

```
/bin/launchctl disable system/com.apple.screensharing
```

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

Note: This will apply to the whole system.

CCI: CCI-000213

Group ID (Vulid): V-259506

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

Rule ID: SV-259506r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002051](#)

Rule Title: The macOS system must disable the TouchID System Settings pane.

Vulnerability Discussion: The System Settings pane for TouchID must be disabled.

Disabling the System Settings pane prevents the users from configuring TouchID.

Check Content:

Verify the macOS system is configured to disable the TouchID System Settings pane with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c "com.apple.Touch-ID-  
Settings.extension"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable the TouchID System Settings pane by installing the "com.apple.systempreferences" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259507

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

Rule ID: SV-259507r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002052](#)

Rule Title: The macOS system must disable the System Settings pane for Wallet and Apple Pay.

Vulnerability Discussion: The System Settings pane for Wallet and Apple Pay must be disabled.

Disabling the System Settings pane prevents the users from configuring Wallet and Apple Pay.

Check Content:

Verify the macOS system is configured to disable the System Settings pane for Wallet and Apple Pay with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c  
"com.apple.WalletSettingsExtension"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable the System Settings pane for Wallet and Apple Pay by installing the "com.apple.systempreferences" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259508

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

Rule ID: SV-259508r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002053](#)

Rule Title: The macOS system must disable the system settings pane for Siri.

Vulnerability Discussion: The System Settings pane for Siri must be hidden.

Hiding the System Settings pane prevents the users from configuring Siri.

Check Content:

Verify the macOS system is configured to disable the system settings pane for Siri with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c com.apple.Siri-  
Settings.extension
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable the system settings pane for Siri by installing the "com.apple.systempreferences" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259509

Group Title: SRG-OS-000366-GPOS-00153

Rule ID: SV-259509r1009592_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-002060](#)

Rule Title: The macOS system must apply gatekeeper settings to block applications from unidentified developers.

Vulnerability Discussion: The information system implements cryptographic mechanisms to authenticate software prior to installation.

Gatekeeper settings must be configured correctly to only allow the system to run applications downloaded from the Mac App Store or 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 in order to run. Digital signatures allow the macOS to verify that the application has not been modified by a malicious third party.

Check Content:

Verify the macOS system is configured to apply gatekeeper settings to block applications from unidentified developers with the following command:

```
/usr/sbin/spctl --status --verbose | /usr/bin/grep -c "developer id enabled"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to apply gatekeeper settings to block applications from unidentified developers with the following command:

```
/usr/sbin/spctl --global-enable; /usr/sbin/spctl --enable
```

CCI: CCI-003992

CCI: CCI-001749

Group ID (Vulid): V-259510

Group Title: SRG-OS-000423-GPOS-00187

Rule ID: SV-259510r958908_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-002062](#)

Rule Title: The macOS system must disable Bluetooth when no approved device is connected.

Vulnerability Discussion: The macOS system must be configured to disable Bluetooth unless an approved device is connected.

[IMPORTANT]

=====

Information system security officers (ISSOs) may make the risk-based decision not to disable Bluetooth to maintain necessary functionality, but they are advised to first fully weigh the potential risks posed to their organization.

=====

Satisfies: SRG-OS-000423-GPOS-00187,SRG-OS-000481-GPOS-00481

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCXBluetooth')\
.objectForKey('DisableBluetooth').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Bluetooth by installing the "com.apple.MCXBluetooth" configuration profiles.

CCI: CCI-002418

Group ID (Vulid): V-259511

Group Title: SRG-OS-000364-GPOS-00151

Rule ID: SV-259511r958796_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002063](#)

Rule Title: The macOS system must disable the guest account.

Vulnerability Discussion: Guest access must be disabled.

Turning off guest access prevents anonymous users from accessing files.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
    let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('DisableGuestAccount'))
```

```
let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('EnableGuestAccount'))
if ( pref1 == true && pref2 == false ) {
    return("true")
} else {
    return("false")
}
}
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable the guest account by installing the "com.apple.MCX" configuration profile.

CCI: CCI-001813

Group ID (Vulid): V-259512

Group Title: SRG-OS-000366-GPOS-00153

Rule ID: SV-259512r1009593_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-002064](#)

Rule Title: The macOS system must enable Gatekeeper.

Vulnerability Discussion: Gatekeeper must be enabled.

Gatekeeper is a security feature that ensures applications are digitally signed by an Apple-issued certificate before they are permitted to run. Digital signatures allow the macOS host to verify that the application has not been modified by a malicious third party.

Administrator users will still have the option to override these settings on a case-by-case basis.

Check Content:

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

```
/usr/sbin/spctl --status | /usr/bin/grep -c "assessments enabled"
```

If the result is not "1", this is a finding.

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

```
/usr/sbin/spctl --global-enable
```

CCI: CCI-003992

CCI: CCI-001749

Group ID (Vulid): V-259513

Group Title: SRG-OS-000480-GPOS-00229

Rule ID: SV-259513r991591_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002066](#)

Rule Title: The macOS system must disable unattended or automatic log on to the system.

Vulnerability Discussion: Automatic logon must be disabled.

When automatic logons are enabled, the default user account is automatically logged on at boot time without prompting the user for a password. Even if the screen is later locked, a malicious user would be able to reboot the computer and find it already logged in. Disabling automatic logons mitigates this risk.

Check Content:

Verify the macOS system is configured to disable unattended or automatic logon to the system with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('com.apple.login.mcx.DisableAutoLoginClient').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable unattended or automatic logon to the system by installing the "com.apple.loginwindow" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-259514

Group Title: SRG-OS-000480-GPOS-00230

Rule ID: SV-259514r991592_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002068](#)

Rule Title: The macOS system must secure user's home folders.

Vulnerability Discussion: The system must be configured to prevent access to other user's home folders.

The default behavior of macOS is to allow all valid users access to the top level of every other user's home folder while restricting access only to the Apple default folders within.

Check Content:

Verify the macOS system is configured so that permissions are set correctly on user home directories with the following command:

```
/usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d ! \( -perm 700 -o -perm 711 \) |
/usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not "0", 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:

```
IFS=$'\n'
for userDirs in $( /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d ! \( -perm 700 -o -
perm 711 \) | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" ); do
```

```
/bin/chmod og-rwx "$userDirs"  
done  
unset IFS
```

CCI: CCI-000366

Group ID (Vulid): V-259515

Group Title: SRG-OS-000324-GPOS-00125

Rule ID: SV-259515r958726_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-002069](#)

Rule Title: The macOS system must require administrator privileges to modify systemwide settings.

Vulnerability Discussion: The system must be configured to require an administrator password in order to modify the systemwide preferences in System Settings.

Some Preference Panes in System Settings contain settings that affect the entire system. Requiring a password to unlock these systemwide settings reduces the risk of a nonauthorized user modifying system configurations.

Check Content:

Verify the macOS system is configured to require administrator privileges to modify systemwide settings with the following command:

```
authDBs=("system.preferences" "system.preferences.energysaver" "system.preferences.network"  
"system.preferences.printing" "system.preferences.sharing" "system.preferences.softwareupdate"  
"system.preferences.startupdisk" "system.preferences.timemachine")  
result="1"  
for section in ${authDBs[@]}; do  
    if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint -xpath 'name(//*[contains(text(),  
"shared")]/following-sibling::*[1])' -) != "false" ]]; then  
        result="0"  
    fi  
done  
echo $result
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to require administrator privileges to modify systemwide settings with the following command:

```
authDBs=("system.preferences" "system.preferences.energysaver" "system.preferences.network"  
"system.preferences.printing" "system.preferences.sharing" "system.preferences.softwareupdate"  
"system.preferences.startupdisk" "system.preferences.timemachine")  
  
for section in ${authDBs[@]}; do  
    /usr/bin/security -q authorizationdb read "$section" > "/tmp/$section.plist"  
    key_value=$(/usr/libexec/PlistBuddy -c "Print :shared" "/tmp/$section.plist" 2>&1)  
    if [[ "$key_value" == *"Does Not Exist"* ]]; then  
        /usr/libexec/PlistBuddy -c "Add :shared bool false" "/tmp/$section.plist"  
    else  
        /usr/libexec/PlistBuddy -c "Set :shared false" "/tmp/$section.plist"  
    fi  
    /usr/bin/security -q authorizationdb write "$section" < "/tmp/$section.plist"
```

done

CCI: CCI-002235

Group ID (Vulid): V-259516

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

Rule ID: SV-259516r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002080](#)

Rule Title: The macOS system must disable Airplay Receiver.

Vulnerability Discussion: Airplay Receiver allows users to send content from another Apple device to be displayed on the screen as it is being played from another device.

Support for Airplay Receiver is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities.

Satisfies: SRG-OS-000095-GPOS-00049,SRG-OS-000300-GPOS-00118

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAirPlayIncomingRequests').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable Airplay Receiver by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

CCI: CCI-001443

Group ID (Vulid): V-259517

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

Rule ID: SV-259517r958400_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002090](#)

Rule Title: The macOS system must disable TouchID for unlocking the device.

Vulnerability Discussion: TouchID enables the ability to unlock a macOS system with a user's fingerprint.

TouchID must be disabled for "Unlocking your Mac" on all macOS devices that are capable of using TouchID.

The system must remain locked until the user establishes access using an authorized identification and authentication method.

Check Content:

Verify the macOS system is configured to disable TouchID for unlocking the device with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowFingerprintForUnlock').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable TouchID for unlocking the device by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000056

Group ID (Vulid): V-259518

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259518r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002100](#)

Rule Title: The macOS system must disable Media Sharing.

Vulnerability Discussion: Media sharing must be disabled.

When Media Sharing is enabled, the computer starts a network listening service that shares the contents of the user's music collection with other users in the same subnet.

The information system must be configured to provide only essential capabilities. Disabling Media Sharing helps prevent the unauthorized connection of devices and the unauthorized transfer of information. Disabling Media Sharing mitigates this risk.

Note: The Media Sharing preference panel will still allow "Home Sharing" and "Share media with guests" to be checked but the service will not be enabled.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
    let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.preferences.sharing.SharingPrefsExtension')
.objectForKey('homeSharingUIStatus'))
    let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.preferences.sharing.SharingPrefsExtension')
.objectForKey('legacySharingUIStatus'))
    let pref3 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.preferences.sharing.SharingPrefsExtension')
.objectForKey('mediaSharingUIStatus'))
    if ( pref1 == 0 && pref2 == 0 && pref3 == 0 ) {
        return("true")
    } else {
```

```
    return("false")
  }
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable media sharing by installing the "com.apple.preferences.sharing.SharingPrefsExtension" configuration profile.

CCI: CCI-000213

Group ID (Vulid): V-259519

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259519r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002110](#)

Rule Title: The macOS system must disable Bluetooth sharing.

Vulnerability Discussion: Bluetooth Sharing must be disabled.

Bluetooth Sharing allows users to wirelessly transmit files between the macOS and Bluetooth-enabled devices, including personally owned cellphones and tablets. A malicious user might introduce viruses or malware onto the system or extract sensitive files via Bluetooth Sharing. When Bluetooth Sharing is disabled, this risk is mitigated.

[NOTE]

=====
The check and fix are for the currently logged on user. To get the currently logged on user, run the following.
[source,bash]

CURRENT_USER=\$(/usr/sbin/scutil <<< "show State:/Users/ConsoleUser" | /usr/bin/awk '/Name :/ && !
/loginwindow/ { print \$3 }')

=====
Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000095-GPOS-00049

Check Content:

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

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost read com.apple.Bluetooth  
PrefKeyServicesEnabled
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system to disable Bluetooth sharing with the following command:

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost write com.apple.Bluetooth  
PrefKeyServicesEnabled -bool false
```

CCI: CCI-000213

Group ID (Vulid): V-259520

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

Rule ID: SV-259520r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002120](#)

Rule Title: The macOS system must disable AppleID and Internet Account modifications.

Vulnerability Discussion: The system must disable account modification.

Account modification includes adding additional or modifying internet accounts in Apple Mail, Calendar, Contacts, in the Internet Account System Setting Pane, or the AppleID System Setting Pane.

This prevents the addition of unauthorized accounts.

[IMPORTANT]

=====

Some organizations may allow the use and configuration of the built-in Mail.app, Calendar.app, and Contacts.app for organizational communication. Information system security officers (ISSOs) may make the risk-based decision not to disable the Internet Accounts System Preference pane to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.

=====

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowAccountModification').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable account modification by installing the "com.apple.applicationaccess" configuration profile.

Group ID (Vulid): V-259521

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

Rule ID: SV-259521r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002130](#)

Rule Title: The macOS system must disable CD/DVD Sharing.

Vulnerability Discussion: CD/DVD Sharing must be disabled.

Check Content:

Verify the macOS system is configured to disable CD/DVD Sharing with the following command:

```
/usr/bin/pgrep -q ODSAgent; /bin/echo $?
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable CD/DVD Sharing with the following command:

```
/bin/launchctl unload /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
```

CCI: CCI-000381

Group ID (Vulid): V-259522

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

Rule ID: SV-259522r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002140](#)

Rule Title: The macOS system must disable content caching service.

Vulnerability Discussion: Content caching must be disabled.

Content caching is a macOS service that helps reduce internet data usage and speed up software installation on Mac computers. It is not recommended for devices furnished to employees to act as a caching server.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowContentCaching').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable content caching service by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259523

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

Rule ID: SV-259523r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002150](#)

Rule Title: The macOS system must disable iCloud desktop and document folder synchronization.

Vulnerability Discussion: The macOS system's ability to automatically synchronize a user's desktop and documents folder to their iCloud Drive must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated file synchronization must be controlled by an organization approved service.

Check Content:

Verify the macOS system is configured to disable iCloud desktop and document folder synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudDesktopAndDocuments').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud desktop and document folder synchronization by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259524

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

Rule ID: SV-259524r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002160](#)

Rule Title: The macOS system must disable iCloud Game Center.

Vulnerability Discussion: This works only with supervised devices (MDM) and allows Apple Game Center to be disabled. The rationale is Game Center is using Apple ID and will share data on AppleID-based services; therefore, Game Center must be disabled. This setting also prohibits the functionality of adding friends to Game Center.

Check Content:

Verify the macOS system is configured to disable iCloud Game Center with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowGameCenter').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Game Center by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259525

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

Rule ID: SV-259525r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002170](#)

Rule Title: The macOS system must disable iCloud Private Relay.

Vulnerability Discussion: Enterprise networks may be required to audit all network traffic by policy; therefore, iCloud Private Relay must be disabled.

Network administrators can also prevent the use of this feature by blocking DNS resolution of mask.icloud.com and mask-h2.icloud.com.

Check Content:

Verify the macOS system is configured to disable the iCloud Private Relay with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowCloudPrivateRelay').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable the iCloud Private Relay by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259526

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

Rule ID: SV-259526r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002180](#)

Rule Title: The macOS system must disable Find My service.

Vulnerability Discussion: The Find My service must be disabled.

A Mobile Device Management (MDM) solution must be used to carry out remote locking and wiping instead of Apple's Find My service.

Apple's Find My service uses a personal AppleID for authentication. Organizations should rely on MDM solutions, which have much more secure authentication requirements, to perform remote lock and remote wipe.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
    let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowFindMyDevice'))
    let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowFindMyFriends'))
    let pref3 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.icloud.managed')\
.objectForKey('DisableFM iCloudSetting'))
    if ( pref1 == false && pref2 == false && pref3 == true ) {
        return("true")
    } else {
        return("false")
    }
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Find My service by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259527

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

Rule ID: SV-259527r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002190](#)

Rule Title: The macOS system must disable password autofill.

Vulnerability Discussion: Password Autofill must be disabled.

macOS allows users to save passwords and use the Password Autofill feature in Safari and compatible apps. To protect against malicious users gaining access to the system, this feature must be disabled to prevent users from being prompted to save passwords in applications.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowPasswordAutoFill').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable password autofill by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259528

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

Rule ID: SV-259528r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002200](#)

Rule Title: The macOS system must disable personalized advertising.

Vulnerability Discussion: Ad tracking and targeted ads must be disabled.

The information system must be configured to provide only essential capabilities. Disabling ad tracking ensures that applications and advertisers are unable to track users' interests and deliver targeted advertisements.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowApplePersonalizedAdvertising').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable personalized advertising by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259529

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

Rule ID: SV-259529r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002210](#)

Rule Title: The macOS system must disable sending Siri and Dictation information to Apple.

Vulnerability Discussion: The ability for Apple to store and review audio of Siri and Dictation interactions must be disabled.

The information system must be configured to provide only essential capabilities. Disabling the submission of Siri and Dictation information will mitigate the risk of unwanted data being sent to Apple.

Check Content:

Verify the macOS system is configured to disable sending Siri and Dictation information to Apple with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.assistant.support')\
.objectForKey('Siri Data Sharing Opt-In Status').js
EOS
```

If the result is not "2", this is a finding.

Fix Text: Configure the macOS system to disable sending Siri and Dictation information to Apple by installing the "com.apple.assistant.support" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259530

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

Rule ID: SV-259530r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002220](#)

Rule Title: The macOS system must enforce on device dictation.

Vulnerability Discussion: Dictation must be restricted to on device only to prevent potential data exfiltration.

The information system must be configured to provide only essential capabilities.

Check Content:

For Intel-based systems, this is not applicable.

Verify the macOS system is configured to enforce on device dictation with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('forceOnDeviceOnlyDictation').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enforce on device dictation by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259531

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

Rule ID: SV-259531r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002230](#)

Rule Title: The macOS system must disable dictation.

Vulnerability Discussion: Dictation must be disabled on Intel-based Macs as the feature On Device Dictation is only available on Apple Silicon devices.

Check Content:

For Apple Silicon-based systems, this is not applicable.

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowDictation').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable dictation by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259532

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

Rule ID: SV-259532r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002240](#)

Rule Title: The macOS system must disable Printer Sharing.

Vulnerability Discussion: Printer Sharing must be disabled.

Check Content:

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

```
/usr/sbin/cupsctl | /usr/bin/grep -c "_share_printers=0"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable Printer Sharing with the following commands:

```
/usr/sbin/cupsctl --no-share-printers
```

```
/usr/bin/lpstat -p | awk '{print $2}' | /usr/bin/xargs -I{} lpadmin -p {} -o printer-is-shared=false
```

CCI: CCI-000381

Group ID (Vulid): V-259533

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

Rule ID: SV-259533r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002250](#)

Rule Title: The macOS system must disable Remote Management.

Vulnerability Discussion: Remote Management must be disabled.

Check Content:

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

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "RemoteDesktopEnabled = 0"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable Remote Management with the following commands:

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -deactivate -stop
```

CCI: CCI-000381

Group ID (Vulid): V-259534

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

Rule ID: SV-259534r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002260](#)

Rule Title: The macOS system must disable the Bluetooth system settings pane.

Vulnerability Discussion: The Bluetooth System Setting pane must be disabled to prevent access to the Bluetooth configuration.

Check Content:

Verify the macOS system is configured to disable the Bluetooth system settings pane with the following

command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
 '//key[text()='DisabledSystemSettings']/following-sibling::*[1]' - | /usr/bin/grep -c com.apple.BluetoothSettings
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to disable the Bluetooth system settings pane by installing the "com.apple.systempreferences" configuration profiles.

CCI: CCI-000381

Group ID (Vulid): V-259535

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

Rule ID: SV-259535r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-002270](#)

Rule Title: The macOS system must disable the iCloud Freeform services.

Vulnerability Discussion: The macOS built-in Freeform.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated calendar synchronization must be controlled by an organization approved service.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\  
.objectForKey('allowCloudFreeform').js  
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable iCloud Freeform services by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259536

Group Title: SRG-OS-000403-GPOS-00182

Rule ID: SV-259536r958868_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003001](#)

Rule Title: The macOS system must issue or obtain public key certificates from an approved service provider.

Vulnerability Discussion: The organization must issue or obtain public key certificates from an organization-approved service provider and ensure only approved trust anchors are in the System Keychain.

Check Content:

Verify the macOS system is configured to issue or obtain public key certificates from an approved service provider with the following command:

```
/usr/bin/security dump-keychain /Library/Keychains/System.keychain | /usr/bin/awk -F'"' '/labl/ {print $4}'
```

If the result does not contain a list of approved certificate authorities, this is a finding.

Fix Text: Configure the macOS system to issue or obtain public key certificates from an approved service provider by obtaining the approved certificates from the appropriate authority and install them to the System Keychain.

CCI: CCI-002470

Group ID (Vulid): V-259537

Group Title: SRG-OS-000071-GPOS-00039

Rule ID: SV-259537r1009594_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003007](#)

Rule Title: The macOS system must require passwords contain a minimum of one numeric character.

Vulnerability Discussion: The macOS must be configured to require at least one numeric character be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Check Content:

Verify the macOS system is configured to require passwords contain a minimum of one numeric character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath '//dict/key[text()="policyIdentifier"]/following-sibling::*[1]/text()' - | /usr/bin/grep "requireAlphanumeric" -c
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to require passwords contain a minimum of one numeric character by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

CCI: CCI-004064

CCI: CCI-000194

Group ID (Vulid): V-259538

Group Title: SRG-OS-000076-GPOS-00044

Rule ID: SV-259538r1038967_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003008](#)

Rule Title: The macOS system must restrict maximum password lifetime to 60 days.

Vulnerability Discussion: The macOS must be configured to enforce a maximum password lifetime limit of at least 60 days.

This rule ensures that users are forced to change their passwords frequently enough to prevent malicious users from gaining and maintaining access to the system.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Check Content:

Verify the macOS system is configured to restrict maximum password lifetime to 60 days with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath  
'//dict/key[text()="policyAttributeExpiresEveryNDays"]/following-sibling::*[1]/text()' -
```

If the result is not "60" or less, this is a finding.

Fix Text: Configure the macOS system to restrict maximum password lifetime to 60 days by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

CCI: CCI-000199

Group ID (Vulid): V-259540

Group Title: SRG-OS-000078-GPOS-00046

Rule ID: SV-259540r1009596_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003010](#)

Rule Title: The macOS system must require a minimum password length of 14 characters.

Vulnerability Discussion: The macOS must be configured to require a minimum of 14 characters be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Check Content:

Verify the macOS system is configured to enforce a minimum 14-character password length with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath 'boolean(//*[contains(text(),"policyAttributePassword matches \"{14,\"}\"])]' -
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enforce a 14-character password length by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

CCI: CCI-004064

CCI: CCI-000205

Group ID (Vulid): V-259541

Group Title: SRG-OS-000266-GPOS-00101

Rule ID: SV-259541r1009597_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003011](#)

Rule Title: The macOS system must require passwords contain a minimum of one special character.

Vulnerability Discussion: The macOS must be configured to require at least one special character be used when a password is created.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ *.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Check Content:

Verify the macOS system is configured to require passwords contain a minimum of one special character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath 'boolean(//*[contains(text(),"policyAttributePassword matches \"{.*[^a-zA-Z0-9].*\}{1,\"}\"])]' -
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to require passwords contain a minimum of one special character by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

CCI: CCI-004064

CCI: CCI-001619

Group ID (Vulid): V-259542
Group Title: SRG-OS-000079-GPOS-00047
Rule ID: SV-259542r958470_rule
Severity: CAT II
Rule Version (STIG-ID): [APPL-14-003012](#)
Rule Title: The macOS system must disable password hints.

Vulnerability Discussion: Password hints must be disabled.

Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\
.objectForKey('RetriesUntilHint').js
EOS
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system to disable password hints by installing the "com.apple.loginwindow" configuration profile.

CCI: CCI-000206

Group ID (Vulid): V-259543
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-259543r991589_rule
Severity: CAT II
Rule Version (STIG-ID): [APPL-14-003013](#)
Rule Title: The macOS system must enable firmware password.

Vulnerability Discussion: A firmware password must be enabled and set.

Single user mode, recovery mode, the Startup Manager, and several other tools are available on macOS by holding the "Option" key down during startup. Setting a firmware password restricts access to these tools.

To set a firmware passcode use the following command:

```
[source,bash]
----
/usr/sbin/firmwarepasswd -setpasswd
----
```

Note: If firmware password or passcode is forgotten, the only way to reset the forgotten password is through the use of a machine specific binary generated and provided by Apple. Schedule a support call and provide proof of purchase before the firmware binary will be generated.

Note: Firmware passwords are not supported on Apple Silicon devices. This rule is only applicable to Intel devices.

Check Content:

For Apple Silicon systems, this is not applicable.

Verify the macOS system is configured with a firmware password with the following command:

```
/usr/sbin/firmwarepasswd -check | /usr/bin/grep -c "Password Enabled: Yes"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system with a firmware password with the following command:

```
/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-259544

Group Title: SRG-OS-000079-GPOS-00047

Rule ID: SV-259544r958470_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003014](#)

Rule Title: The macOS system must remove password hints from user accounts.

Vulnerability Discussion: User accounts must not contain password hints. Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

Check Content:

Verify the macOS system is configured to remove password hints from user accounts with the following command:

```
/usr/bin/dscl . -list /Users hint | /usr/bin/awk '{print $2}' | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system to remove password hints from user accounts with the following command:

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
  /usr/bin/dscl . -delete /Users/$u hint
done
```

CCI: CCI-000206

Group ID (Vulid): V-259545

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

Rule ID: SV-259545r1009598_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003020](#)

Rule Title: The macOS system must enforce smart card authentication.

Vulnerability Discussion: Smart card authentication must be enforced.

The use of smart card credentials facilitates standardization and reduces the risk of unauthorized access.

When enforceSmartCard is set to "true", the smart card must be used for logon, authorization, and unlocking the screen saver.

CAUTION: enforceSmartCard will apply to the whole system. No users will be able to log on with their password unless the profile is removed or a user is exempt from smart card enforcement.

Note: enforceSmartcard requires allowSmartcard to be set to true in order to work.

Satisfies: SRG-OS-000067-GPOS-00035,SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057,SRG-OS-000375-GPOS-00160,SRG-OS-000376-GPOS-00161

Check Content:

Verify the macOS system is configured to enforce multifactor authentication with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')\
.objectForKey('enforceSmartCard').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enforce multifactor authentication by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

CCI: CCI-000186

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-001941

CCI: CCI-004046

CCI: CCI-001953

CCI: CCI-000767

CCI: CCI-000768

CCI: CCI-001948

Group ID (Vulid): V-259546

Group Title: SRG-OS-000068-GPOS-00036

Rule ID: SV-259546r1009599_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003030](#)

Rule Title: The macOS system must allow smart card authentication.

Vulnerability Discussion: Smart card authentication must be allowed.

The use of smart card credentials facilitates standardization and reduces the risk of unauthorized access.

When enabled, the smart card can be used for logon, authorization, and screen saver unlocking.

Satisfies: SRG-OS-000068-GPOS-00036,SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057,SRG-OS-000376-GPOS-00161

Check Content:

Verify the macOS system is configured to allow smart card authentication with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')\
.objectForKey('allowSmartCard').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enforce multifactor authentication by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

CCI: CCI-000187

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-001941

CCI: CCI-001953

CCI: CCI-000767

Group ID (Vulid): V-259547

Group Title: SRG-OS-000105-GPOS-00052

Rule ID: SV-259547r1009600_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003050](#)

Rule Title: The macOS system must enforce multifactor authentication for login.

Vulnerability Discussion: The system must be configured to enforce multifactor authentication.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

IMPORTANT: Modification of Pluggable Authentication Modules (PAM) now requires user authorization or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.

Note: /etc/pam.d/login will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057

Check Content:

Verify the macOS system is configured to enforce multifactor authentication for login with the following command:

```
/usr/bin/grep -Ec '^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_deny.so)' /etc/pam.d/login
```

If the result is not "2", this is a finding.

Fix Text: Configure the macOS system to enforce multifactor authentication for login with the following commands:

```
/bin/cat > /etc/pam.d/login << LOGIN_END
# 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
LOGIN_END
```

```
/bin/chmod 644 /etc/pam.d/login
```

/usr/sbin/chown root:wheel /etc/pam.d/login

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-001941

CCI: CCI-004047

CCI: CCI-000767

CCI: CCI-000768

Group ID (Vulid): V-259548

Group Title: SRG-OS-000105-GPOS-00052

Rule ID: SV-259548r1009601_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003051](#)

Rule Title: The macOS system must enforce multifactor authentication for the su command.

Vulnerability Discussion: The system must be configured such that, when the su command is used, multifactor authentication is enforced.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

IMPORTANT: Modification of Pluggable Authentication Modules (PAM) now requires user authorization or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.

Note: /etc/pam.d/su will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057

Check Content:

Verify the macOS system is configured to enforce multifactor authentication for the su command with the following command:

```
/usr/bin/grep -Ec '^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_rootok.so)'/etc/pam.d/su
```

If the result is not "2", this is a finding.

Fix Text: Configure the macOS system to enforce multifactor authentication for the su command with the following commands:

```
/bin/cat > /etc/pam.d/su << SU_END
```

```
# su: auth account password session
auth      sufficient pam_smartcard.so
auth      required   pam_rootok.so
auth      required   pam_group.so no_warn group=admin,wheel ruser root_only fail_safe
account    required   pam_permit.so
account    required   pam_opendirectory.so no_check_shell
password   required   pam_opendirectory.so
session    required   pam_launchd.so
SU_END
```

```
# Fix new file ownership and permissions
/bin/chmod 644 /etc/pam.d/su
/usr/sbin/chown root:wheel /etc/pam.d/su
```

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-001941

CCI: CCI-004047

CCI: CCI-000767

CCI: CCI-000768

Group ID (Vulid): V-259549

Group Title: SRG-OS-000105-GPOS-00052

Rule ID: SV-259549r1009602_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003052](#)

Rule Title: The macOS system must enforce multifactor authentication for privilege escalation through the sudo command.

Vulnerability Discussion: The system must be configured to enforce multifactor authentication when the sudo command is used to elevate privilege.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

IMPORTANT: Modification of Pluggable Authentication Modules (PAM) now requires user authorization, or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.

Note: /etc/pam.d/sudo will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057

Check Content:

Verify the macOS system is configured to enforce multifactor authentication for privilege escalation through the sudo command with the following command:

```
/usr/bin/grep -Ec '^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_deny.so)' /etc/pam.d/sudo
```

If the result is not "2", this is a finding.

Fix Text: Configure the macOS system to enforce multifactor authentication for privilege escalation through the sudo command with the following commands:

```
/bin/cat > /etc/pam.d/sudo << SUDO_END
# 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
SUDO_END
```

```
/bin/chmod 444 /etc/pam.d/sudo
/usr/sbin/chown root:wheel /etc/pam.d/sudo
```

CCI: CCI-000765

CCI: CCI-000766

CCI: CCI-001941

CCI: CCI-004047

CCI: CCI-000767

CCI: CCI-000768

Group ID (Vulid): V-259550

Group Title: SRG-OS-000069-GPOS-00037

Rule ID: SV-259550r1038909_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003060](#)

Rule Title: The macOS system must require passwords contain a minimum of one lowercase character and one uppercase character.

Vulnerability Discussion: The macOS be configured to require at least one lowercase character and one uppercase character be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Note: The configuration profile generated must be installed from an MDM server.

Satisfies: SRG-OS-000069-GPOS-00037,SRG-OS-000070-GPOS-00038

Check Content:

Verify the macOS system is configured to require passwords contain a minimum of one lowercase character and one uppercase character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath 'boolean(//*[contains(text(),"policyAttributePassword matches \"\"^(?=.*[A-Z])(?=.*[a-z])(?=.*[0-9]).*$\"")])' -
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to require at least one lowercase character and one uppercase character in password complexity by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

CCI: CCI-004064

CCI: CCI-000192

CCI: CCI-000193

Group ID (Vulid): V-259551

Group Title: SRG-OS-000075-GPOS-00043

Rule ID: SV-259551r1038913_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003070](#)

Rule Title: The macOS system must set minimum password lifetime to 24 hours.

Vulnerability Discussion: The macOS must be configured to enforce a minimum password lifetime limit of 24 hours.

This rule discourages users from cycling through their previous passwords to get back to a preferred one.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Check Content:

Verify the macOS system is configured to set minimum password lifetime to 24 hours with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath
```

```
'//dict/key[text()="policyAttributeMinimumLifetimeHours"]/following-sibling::integer[1]/text()' - | /usr/bin/awk  
'{ if ($1 >= 24 ) {print "yes"} else {print "no"}}'
```

If the result is not "yes", this is a finding.

Fix Text: Configure the macOS system to set minimum password lifetime to 24 hours.

This setting may be enforced using local policy or by a directory service.

To set local policy to require a minimum password lifetime, edit the current password policy to contain the following <dict> within the "policyCategoryPasswordContent":

```
[source,xml]  
----  
<dict>  
<key>policyContent</key>  
<string>policyAttributeLastPasswordChangeTime &lt; policyAttributeCurrentTime -  
(policyAttributeMinimumLifetimeHours * 60 * 60)</string>  
<key>policyIdentifier</key>  
<string>Minimum Password Lifetime</string>  
<key>policyParameters</key>  
<dict>  
<key>policyAttributeMinimumLifetimeHours</key>  
<integer>24</integer>  
</dict>  
</dict>  
----
```

After saving the file and exiting to the command prompt, run the following command to load the new policy file, substituting the path to the file in place of "\$pwpolicy_file".

```
[source,bash]  
----  
/usr/bin/pwpolicy setaccountpolicies $pwpolicy_file  
----
```

CCI: CCI-004066

CCI: CCI-000198

Group ID (Vulid): V-259552

Group Title: SRG-OS-000118-GPOS-00060

Rule ID: SV-259552r1038915_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-003080](#)

Rule Title: The macOS system must disable accounts after 35 days of inactivity.

Vulnerability Discussion: The macOS must be configured to disable accounts after 35 days of inactivity.

This rule prevents malicious users from making use of unused accounts to gain access to the system while avoiding detection.

Check Content:

Verify the macOS system is configured to disable accounts after 35 days of inactivity with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --xpath '//dict/key[text()="policyAttributeInactiveDays"]/following-sibling::integer[1]/text()' -
```

If the result is not "35", this is a finding.

Fix Text: Configure the macOS system to disable accounts after 35 days of inactivity with the following command.

This setting may be enforced using local policy or by a directory service.

To set local policy to disable an inactive user after 35 days, edit the current password policy to contain the following <dict> within the "policyCategoryAuthentication":

[source,xml]

```
----
<dict>
<key>policyContent</key>
<string>policyAttributeLastAuthenticationTime &gt; policyAttributeCurrentTime - (policyAttributeInactiveDays
* 24 * 60 * 60)</string>
<key>policyIdentifier</key>
<string>Inactive Account</string>
<key>policyParameters</key>
<dict>
<key>policyAttributeInactiveDays</key>
<integer>35</integer>
</dict>
</dict>
----
```

After saving the file and exiting to the command prompt, run the following command to load the new policy file, substituting the path to the file in place of "\$pwpolicy_file".

[source,bash]

```
----
/usr/bin/pwpolicy setaccountpolicies $pwpolicy_file
----
```

CCI: CCI-003627

CCI: CCI-003628

CCI: CCI-000795

Group ID (Vulid): V-259553

Group Title: SRG-OS-000205-GPOS-00083

Rule ID: SV-259553r958564_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-004001](#)

Rule Title: The macOS system must configure Apple System Log files to be owned by root and group to wheel.

Vulnerability Discussion: The Apple System Logs (ASL) must be owned by root.

ASL logs contain sensitive data about the system and users. If ASL log files are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

Check Content:

Verify the macOS system is configured with Apple System Log files owned by root and group to wheel with the following command:

```
/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system with Apple System Log files owned by root and group to wheel with the following command:

```
/usr/sbin/chown root:wheel $(/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/awk -F":" '!/^root:wheel:/{print $3}')
```

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-259554

Group Title: SRG-OS-000205-GPOS-00083

Rule ID: SV-259554r958564_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-004002](#)

Rule Title: The macOS system must configure Apple System Log files to mode 640 or less permissive.

Vulnerability Discussion: The Apple System Logs (ASL) must be configured to be writable by root and readable only by the root user and group wheel. To achieve this, ASL log files must be configured to mode 640 permissive or less; thereby preventing normal users from reading, modifying, or deleting audit logs. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

Check Content:

Verify the macOS system is configured with Apple System Log files to mode 640 or less permissive with the following command:

```
/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/640/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system with Apple System Log files to mode 640 with the following command:

```
/bin/chmod 640 $(/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk -F":" '{print $2}')
```

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-259555

Group Title: SRG-OS-000373-GPOS-00156

Rule ID: SV-259555r1050789_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-004022](#)

Rule Title: The macOS system must require users to reauthenticate for privilege escalation when using the "sudo" command.

Vulnerability Discussion: The file /etc/sudoers must include a timestamp_timeout of 0.

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 or change user authenticators, 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/sudo -V | /usr/bin/grep -c "Authentication timestamp timeout: 0.0 minutes"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to require reauthentication when using "sudo" with the following command:

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i " '/timestamp_timeout/d' '{}'\ ";  
/bin/echo "Defaults timestamp_timeout=0" >> /etc/sudoers.d/mscp
```

CCI: CCI-004895

CCI: CCI-002038

Group ID (Vulid): V-259556

Group Title: SRG-OS-000205-GPOS-00083

Rule ID: SV-259556r958564_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-004030](#)

Rule Title: The macOS system must configure system log files to be owned by root and group to wheel.

Vulnerability Discussion: The system log files must be owned by root.

System logs contain sensitive data about the system and users. If log files are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

Check Content:

Verify the macOS system is configured with system log files owned by root and group to wheel with the following command:

```
/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system with system log files owned by root and group to wheel with the following command:

```
/usr/sbin/chown root:wheel $(/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk -F":" '!/^root:wheel:/{print $3}')
```

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-259557

Group Title: SRG-OS-000205-GPOS-00083

Rule ID: SV-259557r958564_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-004040](#)

Rule Title: The macOS system must configure system log files to mode 640 or less permissive.

Vulnerability Discussion: The system logs must be configured to be writable by root and readable only by the root user and group wheel. To achieve this, system log files must be configured to mode 640 permissive or less; thereby preventing normal users from reading, modifying, or deleting audit logs. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

Check Content:

Verify the macOS system is configured with system log files set to mode 640 or less permissive with the following command:

```
/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/640/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

Fix Text: Configure the macOS system with system log files set to mode 640 or less permissive with the following command:

```
/bin/chmod 640 $(/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/640/{print $1}' | awk -F":" '!/640/{print $2}')
```

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-259558

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

Rule ID: SV-259558r958752_rule

Severity: CAT III

Rule Version (STIG-ID): [APPL-14-004050](#)

Rule Title: The macOS system must configure install.log retention to 365.

Vulnerability Discussion: The install.log must be configured to require records be kept for an organizational-defined value before deletion, unless the system uses a central audit record storage facility.

Check Content:

Verify the macOS system is configured with install.log retention to 365 with the following command:

```
/usr/sbin/aslmanager -dd 2>&1 | /usr/bin/awk '/\var\log\install.log/ {count++} /Processing module com.apple.install/,Finished/ { for (i=1;i<=NR;i++) { if ($i == "TTL" && $(i+2) >= 365) { ttl="True" }; if ($i == "MAX") { max="True" }}} END{if (count > 1) { print "Multiple config files for /var/log/install, manually remove"} else if (ttl != "True") { print "TTL not configured" } else if (max == "True") { print "Max Size is configured, must be removed" } else { print "Yes" } }'
```

If the result is not "yes", this is a finding.

Fix Text: Configure the macOS system with install.log retention to 365 with the following command:

```
/usr/bin/sed -i " "s/^* file \var\log\install.log.*/* file \var\log\install.log format="\$(\ (Time\)\ (JZ\)) \ $Host \$\ (Sender\)\[\$(PID\)\]: \ $Message' rotate=utc compress file_max=50M size_only ttl=365/g" /etc/asl/com.apple.install
```

Note: If there are multiple configuration files in /etc/asl that are set to process the file /var/log/install.log, these files will have to be manually removed.

CCI: CCI-001849

Group ID (Vulid): V-259559

Group Title: SRG-OS-000373-GPOS-00156

Rule ID: SV-259559r1050789_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-004060](#)

Rule Title: The macOS system must configure sudoers timestamp type.

Vulnerability Discussion: The file /etc/sudoers must be configured to not include a timestamp_type of global or ppid and be configured for timestamp record types of tty.

This rule ensures that the "sudo" command will prompt for the administrator's password at least once in each newly opened terminal window. This prevents a malicious user from taking advantage of an unlocked computer or an abandoned logon session by bypassing the normal password prompt requirement.

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

Check Content:

Verify the macOS system is configured with sudoers timestamp type with the following command:

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/awk -F": " '/Type of authentication timestamp record/{print $2}'
```

If the result is not "tty", this is a finding.

Fix Text: Configure the macOS system with sudoers timestamp type with the following command:

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i " '/timestamp_type/d; /!tty_tickets/d' '{}'\;
```

CCI: CCI-004895

CCI: CCI-002038

Group ID (Vulid): V-259560

Group Title: SRG-OS-000051-GPOS-00024

Rule ID: SV-259560r1038911_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-005001](#)

Rule Title: The macOS system must ensure System Integrity Protection is enabled.

Vulnerability Discussion: System Integrity Protection (SIP) must be enabled.

SIP is vital to protecting the integrity of the system as it prevents malicious users and software from making unauthorized and/or unintended modifications to protected files and folders; ensures the presence of an audit record generation capability for defined auditable events for all operating system components; protects audit tools from unauthorized access, modification, and deletion; restricts the root user account and limits the actions that the root user can perform on protected parts of the macOS; and prevents nonprivileged users from granting other users direct access to the contents of their home directories and folders.

Note: SIP is enabled by default in macOS.

Satisfies: SRG-OS-000051-GPOS-00024,SRG-OS-000054-GPOS-00025,SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000062-GPOS-00031,SRG-OS-000080-GPOS-00048,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-000278-GPOS-00108,SRG-OS-000350-GPOS-00138

Check Content:

Verify the macOS system is configured to enable System Integrity Protection with the following command:

```
/usr/bin/csrutil status | /usr/bin/grep -c 'System Integrity Protection status: enabled.'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to enable "System Integrity Protection" by booting into "Recovery" mode, launch "Terminal" from the "Utilities" menu, and run the following command:

```
/usr/bin/csrutil enable
```

CCI: CCI-000154

CCI: CCI-000158

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000169

CCI: CCI-000213

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-001496

CCI: CCI-001499

CCI: CCI-001876

CCI: CCI-001878

Group ID (Vulid): V-259561

Group Title: SRG-OS-000185-GPOS-00079

Rule ID: SV-259561r958552_rule

Severity: CAT I

Rule Version (STIG-ID): [APPL-14-005020](#)

Rule Title: The macOS system must enforce FileVault.

Vulnerability Discussion: FileVault must be enforced.

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

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 enforce FileVault with the following command:

```
dontAllowDisable=$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')\
.objectForKey('dontAllowFDEDisable').js
EOS
)
fileVault=$(/usr/bin/fdesetup status | /usr/bin/grep -c "FileVault is On.")
if [[ "$dontAllowDisable" == "true" ]] && [[ "$fileVault" == 1 ]]; then
    echo "1"
else
    echo "0"
fi
```

If the result is not "1", this is a finding.

Fix Text: Note: Refer to the FileVault supplemental to implement this rule.

CCI: CCI-001199

CCI: CCI-002475

CCI: CCI-002476

Group ID (Vulid): V-259562

Group Title: SRG-OS-000480-GPOS-00232

Rule ID: SV-259562r991593_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005050](#)

Rule Title: The macOS system must enable the application firewall.

Vulnerability Discussion: The macOS Application Firewall is the built-in firewall that comes with macOS, and it must be enabled.

When the macOS Application Firewall is enabled, the flow of information within the information system and between interconnected systems will be controlled by approved authorizations.

Check Content:

Verify the macOS system is configured to enable the application firewall with the following command:

```
profile="$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')\
.objectForKey('EnableFirewall').js
EOS
)"

plist="$(/usr/bin/defaults read /Library/Preferences/com.apple.alf globalstate 2>/dev/null)"

if [[ "$profile" == "true" ]] && [[ "$plist" =~ [1,2] ]]; then
    echo "true"
else
```

```
    echo "false"  
fi
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enable the application firewall with the following command:

```
/usr/bin/defaults write /Library/Preferences/com.apple.alf globalstate -int 1
```

CCI: CCI-000366

Group ID (Vulid): V-259563

Group Title: SRG-OS-000104-GPOS-00051

Rule ID: SV-259563r958482_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005052](#)

Rule Title: The macOS system must configure login window to prompt for username and password.

Vulnerability Discussion: The login 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 on the login window, which can make it easier for a malicious user to gain access to someone else's account. Requiring users to type in both their username and password mitigates the risk of unauthorized users gaining access to the information system.

Check Content:

Verify the macOS system is configured to prompt for username and password at the login window with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')\  
.objectForKey('SHOWFULLNAME').js  
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to prompt for username and password at the logon window by installing the "com.apple.loginwindow" configuration profile.

CCI: CCI-000764

Group ID (Vulid): V-259564

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

Rule ID: SV-259564r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005054](#)

Rule Title: The macOS system must disable TouchID prompt during Setup Assistant.

Vulnerability Discussion: The prompt for TouchID during Setup Assistant must be disabled.

macOS prompts new users through enabling TouchID during Setup Assistant; this is not essential, and therefore must be disabled to prevent against the risk of individuals electing to enable TouchID to override

organizationwide settings.

Check Content:

Verify the macOS system is configured to disable TouchID prompt during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipTouchIDSetup').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable TouchID prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259565

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

Rule ID: SV-259565r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005055](#)

Rule Title: The macOS system must disable Screen Time prompt during Setup Assistant.

Vulnerability Discussion: The prompt for Screen Time setup during Setup Assistant must be disabled.

Check Content:

Verify the macOS system is configured to disable Screen Time prompt during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipScreenTime').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Screen Time prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259566

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

Rule ID: SV-259566r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005056](#)

Rule Title: The macOS system must disable Unlock with Apple Watch during Setup Assistant.

Vulnerability Discussion: The prompt for Apple Watch unlock setup during Setup Assistant must be disabled.

Disabling Apple watches is a necessary step to ensuring that the information system retains a session lock until the user reestablishes access using an authorized identification and authentication procedures.

Check Content:

Verify the macOS system is configured to disable Unlock with Apple Watch during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')\
.objectForKey('SkipUnlockWithWatch').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to disable Unlock with Apple Watch during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259567

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259567r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005058](#)

Rule Title: The macOS system must disable Handoff.

Vulnerability Discussion: Handoff must be disabled.

Handoff allows users to continue working on a document or project when the user switches from one Apple device to another. Disabling Handoff prevents data transfers to unauthorized devices.

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000095-GPOS-00049,SRG-OS-000300-GPOS-00118

Check Content:

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

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowActivityContinuation').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable handoff by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000213

CCI: CCI-000381

Group ID (Vulid): V-259568

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

Rule ID: SV-259568r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005060](#)

Rule Title: The macOS system must disable proximity-based password sharing requests.

Vulnerability Discussion: Proximity-based password sharing requests must be disabled.

The default behavior of macOS is to allow users to request passwords from other known devices (macOS and iOS). This feature must be disabled to prevent passwords from being shared.

Check Content:

Verify the macOS system is configured to disable proximity-based password sharing requests with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowPasswordProximityRequests').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable proximity-based password sharing requests by installing the "com.apple.applicationaccess" configuration profile.

Group ID (Vulid): V-259569

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

Rule ID: SV-259569r958478_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005061](#)

Rule Title: The macOS system must disable Erase Content and Settings.

Vulnerability Discussion: Erase Content and Settings must be disabled.

Check Content:

Verify the macOS system is configured to disable Erase Content and Settings with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowEraseContentAndSettings').js
EOS
```

If the result is not "false", this is a finding.

Fix Text: Configure the macOS system to disable Erase Content and Settings by installing the

"com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-259570

Group Title: SRG-OS-000080-GPOS-00048

Rule ID: SV-259570r958472_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005070](#)

Rule Title: The macOS system must enable Authenticated Root.

Vulnerability Discussion: Authenticated Root must be enabled.

When Authenticated Root is enabled the macOS is booted from a signed volume that is cryptographically protected to prevent tampering with the system volume.

Note: Authenticated Root is enabled by default on macOS systems.

WARNING: If more than one partition with macOS is detected, the csrutil command will hang awaiting input.

Check Content:

Verify the macOS system is configured to enable authenticated root with the following command:

```
/usr/bin/csrutil authenticated-root | /usr/bin/grep -c 'enabled'
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to enable authenticated root with the following command:

```
/usr/bin/csrutil authenticated-root enable
```

Note: To reenable "Authenticated Root", boot the affected system into "Recovery" mode, launch "Terminal" from the "Utilities" menu, and run the command.

CCI: CCI-000213

Group ID (Vulid): V-259571

Group Title: SRG-OS-000362-GPOS-00149

Rule ID: SV-259571r1009608_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005080](#)

Rule Title: The macOS system must prohibit user installation of software into /users/.

Vulnerability Discussion: Users must not be allowed to install software into /users/.

Allowing users who do not possess explicit privileges to install software presents the risk of untested and potentially malicious software being installed on the system. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceeds the rights of a regular user.

[IMPORTANT]

=====

Apple has deprecated the use of application restriction controls (<https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.newL70>). Using these controls may not work as expected. Third-party software may be required to fulfill the compliance requirements.

Check Content:

Verify the macOS system is configured to prohibit user installation of software into /users/ with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
    let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')\
    .objectForKey('familyControlsEnabled'))
    let pathlist = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')\
    .objectForKey('pathBlackList').js
    for ( let app in pathlist ) {
        if ( ObjC.unwrap(pathlist[app]) == "/Users/" && pref1 == true ){
            return("true")
        }
    }
    return("false")
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to prohibit user installation of software into /users/ by installing the "com.apple.applicationaccess.new" configuration profile.

CCI: CCI-003980

CCI: CCI-001812

Group ID (Vulid): V-259572

Group Title: SRG-OS-000378-GPOS-00163

Rule ID: SV-259572r986236_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005090](#)

Rule Title: The macOS system must authorize USB devices before allowing connection.

Vulnerability Discussion: USB devices connected to a Mac must be authorized.

[IMPORTANT]

This feature is removed if a smart card is paired or smart card attribute mapping is configured.

Check Content:

Verify the macOS system is configured to authorize USB devices before allowing connection with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
  let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowUSBRestrictedMode'))
  if ( pref1 == false ) {
    return("false")
  } else {
    return("true")
  }
}
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to authorize USB devices before allowing connection by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-001958

CCI: CCI-003959

Group ID (Vulid): V-259573

Group Title: SRG-OS-000445-GPOS-00199

Rule ID: SV-259573r958944_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005100](#)

Rule Title: The macOS system must ensure secure boot level set to full.

Vulnerability Discussion: The Secure Boot security setting must be set to full.

Full security is the default Secure Boot setting in macOS. During startup, when Secure Boot is set to full security, the Mac will verify the integrity of the operating system before allowing the operating system to boot.

Note: This will only return a proper result on T2 or Apple Silicon Macs.

Satisfies: SRG-OS-000445-GPOS-00199,SRG-OS-000446-GPOS-00200,SRG-OS-000447-GPOS-00201

Check Content:

Verify the macOS system is configured to ensure secure boot level set to full using the following command:

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "SecureBootLevel = full"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system to ensure secure boot level set to full by booting into Recovery Mode and enable Full Secure Boot.

CCI: CCI-002696

CCI: CCI-002699

Group ID (Vulid): V-259574

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

Rule ID: SV-259574r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005110](#)

Rule Title: The macOS system must enforce enrollment in mobile device management.

Vulnerability Discussion: Users must enroll their Mac in a Mobile Device Management (MDM) software.

User Approved MDM (UAMDM) enrollment or enrollment via Apple Business Manager (ABM)/Apple School Manager (ASM) is required to manage certain security settings. Currently these include:

- * Allowed Kernel Extensions
- * Allowed Approved System Extensions
- * Privacy Preferences Policy Control Payload
- * ExtensibleSingleSignOn
- * FDEFileVault

In macOS 11, UAMDM grants Supervised status on a Mac, unlocking the following MDM features, which were previously locked behind ABM:

- * Activation Lock Bypass
- * Access to Bootstrap Tokens
- * Scheduling Software Updates
- * Query list and delete local users

Check Content:

Verify the macOS system is configured to enforce enrollment in mobile device management with the following command:

```
/usr/bin/profiles status -type enrollment | /usr/bin/awk -F: '/MDM enrollment/ {print $2}' | /usr/bin/grep -c "Yes (User Approved)"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system by ensuring that system is enrolled via UAMDM.

Group ID (Vulid): V-259575

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

Rule ID: SV-259575r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005120](#)

Rule Title: The macOS system must enable recovery lock.

Vulnerability Discussion: A recovery lock password must be enabled and set.

Single user mode, recovery mode, the Startup Manager, and several other tools are available on macOS by holding down specific key combinations during startup. Setting a recovery lock restricts access to these tools.

IMPORTANT: Recovery lock passwords are not supported on Intel devices. This rule is only applicable to Apple Silicon devices.

Check Content:

For non-Apple Silicon systems, this is not applicable.

Verify the macOS system is configured with recovery lock with the following command:

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "IsRecoveryLockEnabled = 1"
```

If the result is not "1", this is a finding.

Fix Text: Configure the macOS system with recovery lock with the SetRecoveryLock command. This can be used to set a Recovery Lock password and must be from the MDM.

CCI: CCI-000366

Group ID (Vulid): V-259576

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

Rule ID: SV-259576r991589_rule

Severity: CAT II

Rule Version (STIG-ID): [APPL-14-005130](#)

Rule Title: The macOS system must enforce installation of XProtect Remediator and Gatekeeper updates automatically.

Vulnerability Discussion: Software Update must be configured to update XProtect Remediator and Gatekeeper updates automatically.

This setting enforces definition updates for XProtect Remediator and Gatekeeper; with this setting in place, new malware and adware that Apple has added to the list of malware or untrusted software will not execute. These updates do not require the computer to be restarted.

<https://support.apple.com/en-us/HT207005>

Note: Software update will automatically update XProtect Remediator and Gatekeeper by default in the macOS.

Check Content:

Verify the macOS system is configured to enforce installation of XProtect Remediator and Gatekeeper updates automatically with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')\
.objectForKey('ConfigDataInstall').js
EOS
```

If the result is not "true", this is a finding.

Fix Text: Configure the macOS system to enforce installation of XProtect Remediator and Gatekeeper updates automatically by installing the "com.apple.SoftwareUpdate" configuration profile.

UNCLASSIFIED