UNCLASSIFIED

Apple macOS 15 (Sequoia) Security Technical Implementation Guide

Version: 1

Release: 8

30 Sep 2026

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 War (DoW) 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-268420
Group Title: SRG-OS-000028-GPOS-00009
Rule ID: SV-268420r1034200_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000001
Rule Title: The macOS system must prevent Apple Watch from terminating a session lock.

Vulnerability Discussion: Apple Watches are not an approved authenticator and their use 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.

NOTE: Unlocking the system with an Apple Watch is not an approved authenticator for U.S. Federal Government usage as it has not been verified to meet the strength requirements outlined in NIST SP 800-63.

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-268421
Group Title: SRG-OS-000028-GPOS-00009
Rule ID: SV-268421r1034203_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000002
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-268422
Group Title: SRG-OS-000028-GPOS-00009
Rule ID: SV-268422r1131177_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000003
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 screen saver 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-268423
Group Title: SRG-OS-000030-GPOS-00011
Rule ID: SV-268423r1034209_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000005
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 absences. 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.

[IMPORTANT]

====
Information system security officers (ISSOs) may make the risk-based decision not to enforce a session lock when a smart token is removed to maintain necessary workflow capabilities, but they are advised to first fully weigh the potential risks posed to their organization.
====

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

Group ID (Vulid): V-268424
Group Title: SRG-OS-000031-GPOS-00012
Rule ID: SV-268424r1034212_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000007
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-268425
Group Title: SRG-OS-000031-GPOS-00012
Rule ID: SV-268425r1034215_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000009
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-000060

Group ID (Vulid): V-268426
Group Title: SRG-OS-000002-GPOS-00002
Rule ID: SV-268426r1268212_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000012
Rule Title: The macOS system must automatically remove or disable temporary or emergency user accounts within 72 hours.

Vulnerability Discussion: The macOS system can 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 login accounts used by system administrators when network or normal login 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 no temporary or emergency accounts are defined on the system, this is not applicable.

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

Check Content:
Verify that 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 no temporary or emergency accounts are 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-268427
Group Title: SRG-OS-000355-GPOS-00143
Rule ID: SV-268427r1131179_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000014
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, SRG-OS-000785-GPOS-00250

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.ManagedClient.preferences" configuration profile.

CCI: CCI-004923

CCI: CCI-004926

CCI: CCI-004922

Group ID (Vulid): V-268428
Group Title: SRG-OS-000021-GPOS-00005

Rule ID: SV-268428r1131182_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000022
Rule Title: The macOS system must limit consecutive failed login attempts to three.

Vulnerability Discussion: The macOS must be configured to limit the number of failed login 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.

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 login 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"}}' | /usr/bin/uniq
```

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

Fix Text: Configure the macOS system to limit consecutive failed login attempts to three by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-000044

CCI: CCI-002238

Group ID (Vulid): V-268429
Group Title: SRG-OS-000023-GPOS-00006
Rule ID: SV-268429r1268215_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000023
Rule Title: The macOS system must display a policy banner at remote login.

Vulnerability Discussion: Remote login service must be configured to display a policy banner at login.

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 login interfaces with human users and are not required when such human interfaces do not exist.

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

Check Content:
Verify the macOS system is configured to display the Standard Mandatory DoW 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 login banner before granting remote access or the banner does not match the Standard Mandatory DoW Notice and Consent Banner, this is a finding.

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

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

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

CCI: CCI-000048

CCI: CCI-000050

Group ID (Vulid): V-269093
Group Title: SRG-OS-000023-GPOS-00006
Rule ID: SV-269093r1268215_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000024
Rule Title: The macOS system must enforce SSH to display a policy banner.

Vulnerability Discussion: SSH must be configured to display a policy banner.

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 login interfaces with human users and are not required when such human interfaces do not exist.

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 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 'banner /etc/banner' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo "banner
/etc/banner" >> "${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-000048

CCI: CCI-000050

Group ID (Vulid): V-268431
Group Title: SRG-OS-000023-GPOS-00006
Rule ID: SV-268431r1268215_rule
Severity: CAT II

Rule Version (STIG-ID): APPL-15-000025
Rule Title: The macOS system must display the Standard Mandatory DoW 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 login 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.rtfd" 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 the command does not return "1", 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.rtfd" and place it in "/Library/Security/".

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

/usr/bin/sudo /bin/chmod 644 /Library/Security/PolicyBanner.rtfd

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-268432
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268432r1034236_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000030
Rule Title: The macOS system must configure audit log files to not contain access control lists (ACLs).

Vulnerability Discussion: The audit log files must not contain 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-268433
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268433r1034239_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000031
Rule Title: The macOS system must configure the audit log folder to not contain access control lists (ACLs).

Vulnerability Discussion: The audit log folder must not contain 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 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-268434
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268434r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000033
Rule Title: The macOS system must disable FileVault automatic login.

Vulnerability Discussion: If FileVault is enabled, automatic login 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 in to the computer once successfully passing FileVault credentials.

NOTE: DisableFDEAutoLogin does not have to be set on Apple Silicon-based macOS systems that are smart card enforced, as smart cards 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-268435
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268435r1131188_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000051
Rule Title: The macOS system must configure SSHD ClientAliveInterval to 900.

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

This 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 look 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-268436
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268436r1034780_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000052
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 that 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 cannot be spoofed. The client alive mechanism is valuable when the client or server depends 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 'clientalivecountmax 1' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo
"clientalivecountmax 1" >> "${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-268437
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268437r1034251_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000053
Rule Title: The macOS system must set login grace time to 30.

Vulnerability Discussion: If SSHD is enabled, it must be configured to wait only 30 seconds before timing out login 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-268438
Group Title: SRG-OS-000033-GPOS-00014
Rule ID: SV-268438r1268222_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-000054
Rule Title: The macOS system must limit SSHD to FIPS-compliant connections.

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

FIPS 140-2/140-3 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets federal requirements.

Operating systems using 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-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp256,sk-ecdsa-sha2-nistp256@openssh.com" "KexAlgorithms ecdh-sha2-nistp256" "MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-256" "PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com" "CASignatureAlgorithms ecdsa-sha2-nistp256,sk-ecdsa-sha2-nistp256@openssh.com")
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:

```
if [ -f /etc/ssh/crypto.conf ] && /usr/bin/grep -q "Include /etc/ssh/crypto.conf" /etc/ssh/sshd_config.d/100-macos.conf 2>/dev/null; then
/bin/ln -fs /etc/ssh/crypto/fips.conf /etc/ssh/crypto.conf
fi

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

fips_sshd_config=("Ciphers aes128-gcm@openssh.com" "HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "HostKeyAlgorithms ecdsa-sha2-nistp256-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp256,sk-ecdsa-sha2-nistp256@openssh.com" "KexAlgorithms ecdh-sha2-nistp256" "MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-256" "PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com" "CASignatureAlgorithms ecdsa-sha2-nistp256,sk-ecdsa-sha2-nistp256@openssh.com")
sshd_config=$(/usr/sbin/sshd -G)
for config in $fips_sshd_config; do
if ! echo $sshd_config | /usr/bin/grep -q -i "$config" 2>/dev/null; then
/usr/bin/grep -qxF "$config" "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo "$config" >>
"${include_dir}01-mscp-sshd.conf"
fi
done

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-000068

CCI: CCI-000803

CCI: CCI-001453

CCI: CCI-002890

CCI: CCI-003123

CCI: CCI-002450

CCI: CCI-002421

Group ID (Vulid): V-268439
Group Title: SRG-OS-000033-GPOS-00014
Rule ID: SV-268439r1268222_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-000057
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 140-3 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets federal requirements.

Operating systems using 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=("Ciphers aes128-gcm@openssh.com" "HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "HostKeyAlgorithms ecdsa-sha2-nistp256-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp256,sk-ecdsa-sha2-nistp256@openssh.com" "KexAlgorithms ecdh-sha2-nistp256" "MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-256" "PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-

```
v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com" "CASignatureAlgorithms ecdsa-sha2-
nistp256,sk-ecdsa-sha2-nistp256@openssh.com")
total=0
ret="pass"
for config in $fips_ssh_config; do
if [[ "$ret" == "fail" ]]; then
break
fi
for u in $(/usr/bin/dscl . list /users shell | /usr/bin/egrep -v '(^_)|(root)|(/usr/bin/false)' | /usr/bin/awk '{print $1}');
do
sshCheck=$(/usr/bin/sudo -u $u /usr/bin/ssh -G . | /usr/bin/grep -ci "$config")
if [[ "$sshCheck" == "0" ]]; then
ret="fail"
break
fi
done
done
echo $ret
```

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

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

```
if [ -f /etc/ssh/crypto.conf ] && /usr/bin/grep -q "Include /etc/ssh/crypto.conf" /etc/ssh/ssh_config.d/100-
macos.conf 2>/dev/null; then
/bin/ln -fs /etc/ssh/crypto/fips.conf /etc/ssh/crypto.conf
fi
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/ssh_config | /usr/bin/tr -d '*')

fips_ssh_config=("Ciphers aes128-gcm@openssh.com" "HostbasedAcceptedAlgorithms ecdsa-sha2-
nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "HostKeyAlgorithms ecdsa-sha2-nistp256-cert-
v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp256,sk-ecdsa-sha2-
nistp256@openssh.com" "KexAlgorithms ecdh-sha2-nistp256" "MACs hmac-sha2-256-
etm@openssh.com,hmac-sha2-256" "PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-
v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com" "CASignatureAlgorithms ecdsa-sha2-
nistp256,sk-ecdsa-sha2-nistp256@openssh.com")
for ssh_config in $fips_ssh_config; do
ssh_setting=$(echo $ssh_config | /usr/bin/cut -d " " -f1)
/usr/bin/grep -qEi "^$ssh_setting" "${include_dir}01-mscp-ssh.conf" && /usr/bin/sed -i ""
"s/^$ssh_setting.*/${ssh_config}/" "${include_dir}01-mscp-ssh.conf" || echo "$ssh_config" >>
"${include_dir}01-mscp-ssh.conf"
for u in $(/usr/bin/dscl . list /users shell | /usr/bin/egrep -v '(^_)|(root)|(/usr/bin/false)' | /usr/bin/awk '{print $1}');
do
config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1)
configfiles=$(echo "$config" | /usr/bin/awk '/Reading configuration data/ {print $NF}'| /usr/bin/tr -d '\r')
configarray=( ${(f)configfiles} )
if ! echo $config | /usr/bin/grep -q -i "$ssh_config" ; then
for c in $configarray; do
if [[ "$c" == "/etc/ssh/crypto.conf" ]]; then
continue
fi

/usr/bin/sudo -u $u /usr/bin/grep -qEi "^$ssh_setting" "$c" && /usr/bin/sed -i ""
```

```
"s/^$ssh_setting.*/${ssh_config}/I" "$c"
if [[ "$c" =~ ".ssh/config" ]]; then
if /usr/bin/grep -qEi "$ssh_setting" "$c" 2> /dev/null; then
old_file=$(cat ~$u/.ssh/config)
echo "$ssh_config" > ~$u/.ssh/config
echo "$old_file" >> ~$u/.ssh/config
fi
fi
done
fi
done
done
```

CCI: CCI-000068

CCI: CCI-000803

CCI: CCI-001453

CCI: CCI-002450

CCI: CCI-002421

Group ID (Vulid): V-268440
Group Title: SRG-OS-000021-GPOS-00005
Rule ID: SV-268440r1131197_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000060
Rule Title: The macOS system must set account lockout time to 15 minutes.

Vulnerability Discussion: The macOS system must be configured to enforce a lockout time of at least 15 minutes when the maximum number of failed login 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"}}' | /usr/bin/uniq
```

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.

CCI: CCI-000044

CCI: CCI-002238

Group ID (Vulid): V-268441
Group Title: SRG-OS-000029-GPOS-00010
Rule ID: SV-268441r1131199_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000070
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-268442
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-268442r1131200_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000090
Rule Title: The macOS system must disable login to other users' active and locked sessions.

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

WARNING: This rule may cause issues when platformSSO is configured.

macOS has a privilege that can be granted to any user that will allow that user to unlock active users' sessions. Disabling the administrator's and/or user's ability to log in to another user's active and locked session prevents

unauthorized people from viewing potentially sensitive and/or personal information.

Note: Configuring this setting will change the user experience and disable TouchID from unlocking the screen saver. To restore the user experience and allow TouchID to unlock the screen saver, run "/usr/bin/sudo /usr/bin/defaults write /Library/Preferences/com.apple.loginwindow screenUnlockMode -int 1". This setting can also be deployed with a configuration profile.

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

Check Content:
Verify the macOS system is configured to disable login to other users' 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 users' 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

Group ID (Vulid): V-268443
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-268443r1034269_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000100
Rule Title: The macOS system must disable root login.

Vulnerability Discussion: To assure 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

Group ID (Vulid): V-268444
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268444r1131203_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000110
Rule Title: The macOS system must configure the SSH ServerAliveInterval 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 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 to 900 with the following command:

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

ssh_config_string=("ServerAliveInterval 900")
for ssh_config in $ssh_config_string; do
ssh_setting=$(echo $ssh_config | /usr/bin/cut -d " " -f1)
/usr/bin/grep -qEi "^$ssh_setting" "${include_dir}01-mscp-ssh.conf" && /usr/bin/sed -i ""
"s/^$ssh_setting.*/${ssh_config}/" "${include_dir}01-mscp-ssh.conf" || echo "$ssh_config" >>
"${include_dir}01-mscp-ssh.conf"
for u in $(/usr/bin/dscl . list /users shell | /usr/bin/egrep -v '(^_)|(root)|(/usr/bin/false)' | /usr/bin/awk '{print $1}');
do
config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1)
configfiles=$(echo "$config" | /usr/bin/awk '/Reading configuration data/ {print $NF}'| /usr/bin/tr -d '\r')
```

```
configarray=( ${(f)configfiles} )
if ! echo $config | /usr/bin/grep -q -i "$ssh_config" ; then
for c in $configarray; do
if [[ "$c" == "/etc/ssh/crypto.conf" ]]; then
continue
fi

/usr/bin/sudo -u $u /usr/bin/grep -qEi "^$ssh_setting" "$c" && /usr/bin/sed -i ""
"s/^$ssh_setting.*/${ssh_config}/I" "$c"
if [[ "$c" =~ ".ssh/config" ]]; then
if /usr/bin/grep -qEi "$ssh_setting" "$c" 2> /dev/null; then
old_file=$(cat ~$u/.ssh/config)
echo "$ssh_config" > ~$u/.ssh/config
echo "$old_file" >> ~$u/.ssh/config
fi
fi
done
fi
done
done
```

CCI: CCI-001133

Group ID (Vulid): V-268445
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268445r1034275_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000120
Rule Title: The macOS system must configure SSHD channel timeout to 900.

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

This will set the timeout 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 "=" '/channeltimeout session:*/{print $2}'
```

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

Fix Text: Configure the macOS system to set the SSHD ChannelTimeout 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 'channeltimeout session:*=900' "${include_dir}01-mscp-sshd.conf" 2>/dev/null || echo "channeltimeout session:*=900" >> "${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-268446
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268446r1034278_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000130
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
  /bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

CCI: CCI-001133

CCI: CCI-002361

Group ID (Vulid): V-268447
Group Title: SRG-OS-000163-GPOS-00072
Rule ID: SV-268447r1131206_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000140
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 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. 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:

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

```
ssh_config=("ServerAliveCountMax 0")

ssh_setting=$(echo $ssh_config | /usr/bin/cut -d " " -f1)
/usr/bin/grep -qEi "^$ssh_setting" "${include_dir}01-mscp-ssh.conf" && /usr/bin/sed -i ""
"s/^$ssh_setting.*/${ssh_config}/" "${include_dir}01-mscp-ssh.conf" || echo "$ssh_config" >>
"${include_dir}01-mscp-ssh.conf"
for u in $(/usr/bin/dscl . list /users shell | /usr/bin/egrep -v '(^_)|(root)|(/usr/bin/false)' | /usr/bin/awk '{print $1}');
do
config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1)
configfiles=$(echo "$config" | /usr/bin/awk '/Reading configuration data/ {print $NF}'| /usr/bin/tr -d '\r')
configarray=( ${(f)configfiles} )
if ! echo $config | /usr/bin/grep -q -i "$ssh_config" ; then
for c in $configarray; do
if [[ "$c" == "/etc/ssh/crypto.conf" ]]; then
continue
fi

/usr/bin/sudo -u $u /usr/bin/grep -qEi "^$ssh_setting" "$c" && /usr/bin/sed -i ""
"s/^$ssh_setting.*/${ssh_config}/I" "$c"
if [[ "$c" =~ ".ssh/config" ]]; then
if /usr/bin/grep -qEi "$ssh_setting" "$c" 2> /dev/null; then
old_file=$(cat ~$u/.ssh/config)
echo "$ssh_config" > ~$u/.ssh/config
echo "$old_file" >> ~$u/.ssh/config
fi
fi
done
fi
done
```

CCI: CCI-001133

Group ID (Vulid): V-268448
Group Title: SRG-OS-000279-GPOS-00109
Rule ID: SV-268448r1034284_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000160
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 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.

CCI: CCI-002361

Group ID (Vulid): V-268449
Group Title: SRG-OS-000355-GPOS-00143
Rule ID: SV-268449r1268019_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000170
Rule Title: The macOS system must be configured to use an authorized time server.

Vulnerability Discussion: An approved time server must be the only server configured for use. As of macOS 10.13, only one time server is supported.

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 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 that is synchronized with redundant USNO time servers as designated for the appropriate DoW 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

Group ID (Vulid): V-268450
Group Title: SRG-OS-000355-GPOS-00143

Rule ID: SV-268450r1038944_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000180
Rule Title: The macOS system must enable the 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, SRG-OS-000785-GPOS-00250

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

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

NOTE: The service "timed" cannot be unloaded or loaded while System Integrity Protection (SIP) is enabled.

CCI: CCI-004923

CCI: CCI-004926

CCI: CCI-004922

Group ID (Vulid): V-268451
Group Title: SRG-OS-000064-GPOS-00033
Rule ID: SV-268451r1131208_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-000190
Rule Title: The macOS system must configure sudo to log events.

Vulnerability Discussion: Sudo must be configured to log privilege escalation.

Without logging privilege escalation, it is difficult to identify attempted attacks because no audit trail is available for forensic investigation.

Check Content:
Verify the macOS system is configured to log privilege escalation with the following command:

/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Log when a command is allowed by sudoers"

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

Fix Text: Configure the macOS system to log privilege escalation with the following command:

/usr/bin/find /etc/sudoers* -type f -exec sed -i " '/^Defaults[[:blank:]]*\!log_allowed/s/^/# /' '{}' \;
/bin/echo "Defaults log_allowed" >> /etc/sudoers.d/mscp

CCI: CCI-000172

Group ID (Vulid): V-268452
Group Title: SRG-OS-000004-GPOS-00004
Rule ID: SV-268452r1131210_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001001
Rule Title: The macOS system must be configured to audit all administrative action events.

Vulnerability Discussion: The auditing system must be configured to flag administrative action (ad) events.

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).

The information system audits the execution of privileged functions.

Note: Changing the line "43127:AUE_MAC_SYSCALL:mac_syscall(2):ad" to "43127:AUE_MAC_SYSCALL:mac_syscall(2):zz" in the file /etc/security/audit_event is recommended. This will prevent sandbox violations from being audited by 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-000303-GPOS-00120, 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 the result is not "1", 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-001403

CCI: CCI-001404

CCI: CCI-001405

CCI: CCI-002130

CCI: CCI-002234

CCI: CCI-003938

CCI: CCI-002884

CCI: CCI-000172

Group ID (Vulid): V-268453
Group Title: SRG-OS-000032-GPOS-00013
Rule ID: SV-268453r1268219_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001002
Rule Title: The macOS system must be configured to audit all login and logout 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 service account. The attacker must attempt to change to another user account with normal or elevated privileges to proceed. Auditing both successful and unsuccessful attempts to switch to another user account (by way of monitoring login and logout events) mitigates this risk.

The information system monitors login and logout 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 login and logout 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 login and logout events with the following command:

```
/usr/bin/grep -qE "^flags.*[^-]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-268454
Group Title: SRG-OS-000037-GPOS-00015
Rule ID: SV-268454r1034302_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001003
Rule Title: The macOS system must enable security auditing.

Vulnerability Discussion: The information system must be configured to generate audit records.

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 NOT enabled by default on macOS Sequoia.

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-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, SRG-OS-000755-GPOS-00220

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

```
LAUNCHD_RUNNING=$(/bin/launchctl list | /usr/bin/grep -c com.apple.auditd)
AUDITD_RUNNING=$(/usr/sbin/audit -c | /usr/bin/grep -c "AUC_AUDITING")
if [[ $LAUNCHD_RUNNING == 1 ]] && [[ -e /etc/security/audit_control ]] && [[ $AUDITD_RUNNING == 1 ]]; 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:

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

/bin/launchctl enable system/com.apple.auditd
/bin/launchctl bootstrap system /System/Library/LaunchDaemons/com.apple.auditd.plist
/usr/sbin/audit -i
```

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000159

CCI: CCI-001464

CCI: CCI-001487

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-001914

CCI: CCI-001889

CCI: CCI-001890

CCI: CCI-003938

CCI: CCI-002884

CCI: CCI-000172

CCI: CCI-004188

Group ID (Vulid): V-268455
Group Title: SRG-OS-000047-GPOS-00023
Rule ID: SV-268455r1038966_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001010
Rule Title: The macOS system must be configured 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.

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: ahlt,argv/' /etc/security/audit_control; /usr/sbin/audit -s
```

CCI: CCI-000140

Group ID (Vulid): V-268456
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268456r1034308_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001012
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 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 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-268457
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268457r1034311_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001013
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 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 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-268458
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268458r1034314_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001014
Rule Title: The macOS system must configure the 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-268459
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268459r1034317_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001015
Rule Title: The macOS system must configure the audit log folders 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 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-268460
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268460r1034320_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001016
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 to prevent 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-268461
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268461r1034323_rule
Severity: CAT II

Rule Version (STIG-ID): APPL-15-001017
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 to prevent 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-268462
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268462r1034326_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001020
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 because no audit trail is 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

Group ID (Vulid): V-268463
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268463r1034329_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001021

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 attempt to modify a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks because no audit trail is 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 '/^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

Group ID (Vulid): V-268464
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268464r1034332_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001022
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 because no audit trail is 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-000461-GPOS-00205, SRG-OS-000463-GPOS-00207, 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-000163

CCI: CCI-000164

CCI: CCI-000172

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-003938

CCI: CCI-002884

Group ID (Vulid): V-268465
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268465r1034335_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001023
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 because no audit trail is 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 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-000163

CCI: CCI-000164

CCI: CCI-000172

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-003938

CCI: CCI-002884

Group ID (Vulid): V-269094
Group Title: SRG-OS-000365-GPOS-00152
Rule ID: SV-269094r1034757_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001024
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 because no audit trail is available for forensic investigation.

Satisfies: SRG-OS-000365-GPOS-00152, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, 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-003938

CCI: CCI-000172

Group ID (Vulid): V-268467
Group Title: SRG-OS-000341-GPOS-00132
Rule ID: SV-268467r1034341_rule
Severity: CAT III
Rule Version (STIG-ID): APPL-15-001029
Rule Title: The macOS system must configure audit retention to seven days.

Vulnerability Discussion: The audit service must be configured to require that 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 to set 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-268468
Group Title: SRG-OS-000046-GPOS-00022
Rule ID: SV-268468r1034344_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001030
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

CCI: CCI-001855

Group ID (Vulid): V-268469
Group Title: SRG-OS-000047-GPOS-00023
Rule ID: SV-268469r1038966_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001031
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-268470

Group Title: SRG-OS-000365-GPOS-00152
Rule ID: SV-268470r1034350_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001044
Rule Title: The macOS system must be configured 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 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 login 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 login 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-003938

CCI: CCI-002884

CCI: CCI-000172

Group ID (Vulid): V-268471
Group Title: SRG-OS-000066-GPOS-00034
Rule ID: SV-268471r1034353_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001060
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

Group ID (Vulid): V-268472
Group Title: SRG-OS-000109-GPOS-00056
Rule ID: SV-268472r1034356_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001100
Rule Title: The macOS system must disable root login 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

Group ID (Vulid): V-268473
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268473r1034359_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001110
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 manipulating audit log configurations.

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-268474
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268474r1034362_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001120
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 manipulating audit log configurations.

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-268475
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-268475r1034365_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001130
Rule Title: The macOS system must configure audit_control owner 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.

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

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 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 result is 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-269095
Group Title: SRG-OS-000057-GPOS-00027
Rule ID: SV-269095r1034760_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-001140
Rule Title: The macOS system must configure audit_control to not contain access control lists (ACLs).

Vulnerability Discussion: /etc/security/audit_control must not contain 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 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

CCI: CCI-001495

Group ID (Vulid): V-268477
Group Title: SRG-OS-000067-GPOS-00035
Rule ID: SV-268477r1034371_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-001150
Rule Title: The macOS system must disable password authentication for SSH.

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

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-001941

CCI: CCI-000877

CCI: CCI-004046

Group ID (Vulid): V-268478
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268478r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002001
Rule Title: The macOS system must disable Server Message Block (SMB) sharing.

Vulnerability Discussion: Support for SMB file sharing is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable SMB 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 SMB 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-268479
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268479r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002003
Rule Title: The macOS system must disable Network File System (NFS) service.

Vulnerability Discussion: Support for NFS services is nonessential and, therefore, must be disabled. Enabling

any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable NFS 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 NFS 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-268480
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268480r1034380_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002004
Rule Title: The macOS system must disable Location Services.

Vulnerability Discussion: Location Services must be disabled.

The information system must be configured to provide only essential capabilities. Disabling Location Services helps prevent unauthorized connection of devices, transfer of information, and 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;
pid=$(/bin/launchctl list | /usr/bin/awk '/com.apple.locationd/ { print $1 }')
kill -9 $pid
```

CCI: CCI-000381

Group ID (Vulid): V-268481
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268481r1034383_rule

Severity: CAT II
Rule Version (STIG-ID): APPL-15-002005
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-268482
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268482r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002006
Rule Title: The macOS system must disable Unix-to-Unix Copy Protocol (UUCP) service.

Vulnerability Discussion: The system must not have the UUCP service active.

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

NOTE: UUCP service is disabled at startup by default with macOS.

Check Content:
Verify the macOS system is configured to disable UUCP 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 UUCP 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-268483
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268483r1034389_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002007
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 unauthorized connection of devices, transfer of information, and 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-268484
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268484r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002008
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 is disabled at startup by default with 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-268485
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268485r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002009
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-268486
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268486r1034398_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002010
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-268487
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268487r1034401_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002012
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-268488
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268488r1034404_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002013
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-268489
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268489r1034407_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002014
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-268490
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268490r1034410_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002015
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-268491
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268491r1034413_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002016
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-268492
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268492r1034416_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002017
Rule Title: The macOS system must disable the camera.

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

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

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 video teleconference (VTC) suites 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-268493
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268493r1034419_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002020
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. Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable 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-268494
Group Title: SRG-OS-000205-GPOS-00083
Rule ID: SV-268494r1131212_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002021
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.SubmitDiagInfo" configuration profile.

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-268495
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268495r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002022
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 unauthorized connection of devices, transfer of information, and 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

CCI: CCI-000382

Group ID (Vulid): V-269096
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-269096r1131214_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002023
Rule Title: The macOS system must disable sending audio recordings and transcripts to Apple.

Vulnerability Discussion: The ability for Apple to store and review audio recordings and transcripts of vocal shortcuts and voice control interactions must be disabled.

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

Check Content:
Verify the macOS system is configured to disable sending audio recordings and transcripts with the following command:

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

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

Fix Text: Configure the macOS system to disable sending audio recordings and transcripts by installing the "com.apple.accessibility" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-269566
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-269566r1131216_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002024
Rule Title: The macOS system must disable sending search data from Spotlight to Apple.

Vulnerability Discussion: Sending data to Apple to help improve search must be disabled.

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

Check Content:
Verify the macOS system is configured to disable sending search data from Spotlight with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.assistant.support')\
.objectForKey('Search Queries Data Sharing Status').js
EOS
```

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

Fix Text: Configure the macOS system to disable sending search data from Spotlight by installing the "com.apple.assistant.support" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268496
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268496r1034428_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002035
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. This can mislead new users into thinking they need to create Apple ID accounts upon their first login.

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.

CCI: CCI-000381

Group ID (Vulid): V-268497
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268497r1034431_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002036
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 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-268498
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268498r1034434_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002037
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 with more control over their data storage.

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-268499

Group Title: SRG-OS-000074-GPOS-00042
Rule ID: SV-268499r1034437_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-002038
Rule Title: The macOS system must disable Trivial File Transfer Protocol (TFTP) service.

Vulnerability Discussion: If the system does not require 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 unauthorized transfer of information.

NOTE: TFTP service is disabled at startup by default with macOS.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000080-GPOS-00048

Check Content:
Verify the macOS system is configured to disable TFTP 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 TFTP 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-268500
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268500r1034440_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002039
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 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-268501
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268501r1034443_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002040
Rule Title: The macOS system must disable iCloud Keychain Sync.

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 Sync 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 Sync by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268502
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268502r1034446_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002041
Rule Title: The macOS system must disable iCloud Document Sync.

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 Sync 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 Sync by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268503
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268503r1034449_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002042
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-268504
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268504r1034452_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002043
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-268505
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268505r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002050
Rule Title: The macOS system must disable Screen Sharing and Apple Remote Desktop.

Vulnerability Discussion: Support for both Screen Sharing and Apple Remote Desktop is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling Screen Sharing and Apple Remote Desktop helps prevent unauthorized connection of devices, transfer of information, and 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-268506
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268506r1034458_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002052
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. Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable the 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-268507
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268507r1034461_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002053
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 users from configuring Siri. Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable the 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-268508
Group Title: SRG-OS-000366-GPOS-00153
Rule ID: SV-268508r1268241_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-002060
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 allow the system to run only 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 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 commands:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systempolicy.control')\
.objectForKey('AllowIdentifiedDevelopers'))
let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.systempolicy.control')\
.objectForKey('EnableAssessment'))
if ( pref1 == true && pref2 == true ) {
return("true")
} else {
return("false")
}
}
EOS
```

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

Fix Text: Configure the macOS system to apply gatekeeper settings to block applications from unidentified developers by installing the "com.apple.systempolicy.control" configuration profile.

CCI: CCI-003992

Group ID (Vulid): V-268509
Group Title: SRG-OS-000423-GPOS-00187
Rule ID: SV-268509r1034467_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-002062
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 profile.

CCI: CCI-002418

Group ID (Vulid): V-268510
Group Title: SRG-OS-000364-GPOS-00151
Rule ID: SV-268510r1131221_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002063
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-268511
Group Title: SRG-OS-000366-GPOS-00153
Rule ID: SV-268511r1268241_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-002064
Rule Title: The macOS system must enable gatekeeper.

Vulnerability Discussion: Gatekeeper must be enabled.

Gatekeeper is a security feature that ensures that applications are digitally signed by an Apple-issued certificate before they are permitted to run. Digital signatures allow the macOS host to verify 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/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.systempolicy.control')\
.objectForKey('EnableAssessment').js
EOS
```

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

Fix Text: Configure the macOS system to enable gatekeeper by installing the "com.apple.systempolicy.control" configuration profile.

CCI: CCI-003992

Group ID (Vulid): V-268512
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-268512r1034476_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-002066
Rule Title: The macOS system must disable unattended or automatic login to the system.

Vulnerability Discussion: Automatic login must be disabled.

When automatic logins 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 logins mitigates this risk.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000480-GPOS-00229

Check Content:
Verify the macOS system is configured to disable unattended or automatic login 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 login to the system by installing the "com.apple.loginwindow" configuration profile.

CCI: CCI-000764

CCI: CCI-000366

Group ID (Vulid): V-268513
Group Title: SRG-OS-000480-GPOS-00230
Rule ID: SV-268513r1131226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002068
Rule Title: The macOS system must secure users' home folders.

Vulnerability Discussion: The system must be configured to prevent access to other users' 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.

Satisfies: SRG-OS-000480-GPOS-00230, SRG-OS-000480-GPOS-00228

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-268514
Group Title: SRG-OS-000324-GPOS-00125
Rule ID: SV-268514r1131229_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-002069
Rule Title: The macOS system must require an administrator password to modify systemwide preferences.

Vulnerability Discussion: The system must be configured to require an administrator password 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 an unauthorized 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
if [[ $(security -q authorizationdb read "$section" | /usr/bin/xmllint -xpath '//*[contains(text(),
"group")]/following-sibling::*[1]/text()' - ) != "admin" ]]; then
result="0"
fi
if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint -xpath 'name(//*[contains(text(),
"authenticate-user")]/following-sibling::*[1])' -) != "true" ]]; then
result="0"
fi
if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint -xpath 'name(//*[contains(text(),
"session-owner")]/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"

class_key_value=$(usr/libexec/PlistBuddy -c "Print :class" "/tmp/$section.plist" 2>&1)
if [[ "$class_key_value" == *"Does Not Exist"* ]]; then
/usr/libexec/PlistBuddy -c "Add :class string user" "/tmp/$section.plist"
else
/usr/libexec/PlistBuddy -c "Set :class user" "/tmp/$section.plist"
fi

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

auth_user_key=$(/usr/libexec/PlistBuddy -c "Print :authenticate-user" "/tmp/$section.plist" 2>&1)
if [[ "$auth_user_key" == *"Does Not Exist"* ]]; then
/usr/libexec/PlistBuddy -c "Add :authenticate-user bool true" "/tmp/$section.plist"
else
/usr/libexec/PlistBuddy -c "Set :authenticate-user true" "/tmp/$section.plist"
fi

session_owner_key=$(/usr/libexec/PlistBuddy -c "Print :session-owner" "/tmp/$section.plist" 2>&1)
if [[ "$session_owner_key" == *"Does Not Exist"* ]]; then
/usr/libexec/PlistBuddy -c "Add :session-owner bool false" "/tmp/$section.plist"
else
/usr/libexec/PlistBuddy -c "Set :session-owner false" "/tmp/$section.plist"
fi

group_key=$(usr/libexec/PlistBuddy -c "Print :group" "/tmp/$section.plist" 2>&1)
if [[ "$group_key" == *"Does Not Exist"* ]]; then
/usr/libexec/PlistBuddy -c "Add :group string admin" "/tmp/$section.plist"
else
/usr/libexec/PlistBuddy -c "Set :group admin" "/tmp/$section.plist"
fi

/usr/bin/security -q authorizationdb write "$section" < "/tmp/$section.plist"
done
```

CCI: CCI-002235

Group ID (Vulid): V-268515
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268515r1034485_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002080
Rule Title: The macOS system must disable Airplay Receiver.

Vulnerability Discussion: Airplay Receiver allows users to send content from one 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-268516
Group Title: SRG-OS-000028-GPOS-00009
Rule ID: SV-268516r1034488_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002090
Rule Title: The macOS system must disable TouchID for unlocking the device.

Vulnerability Discussion: TouchID enables the ability to unlock a Mac 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.

NOTE: TouchID is not an approved biometric authenticator for U.S. Federal Government use as it has not been verified to meet the strength requirements outlined in NIST SP 800-63.

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-268517
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268517r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002100
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 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 commands:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowMediaSharing'))
let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')\
.objectForKey('allowMediaSharingModification'))
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 Media Sharing by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000213

Group ID (Vulid): V-268518
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268518r1268226_rule
Severity: CAT II

Rule Version (STIG-ID): APPL-15-002110
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 in user. To get the currently logged in 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 commands:

```
CURRENT_USER=$( /usr/sbin/scutil <<< "show State:/Users/ConsoleUser" | /usr/bin/awk '/Name :/ && ! /loginwindow/ { print $3 }' )
/usr/bin/sudo -u "$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 commands:

```
CURRENT_USER=$( /usr/sbin/scutil <<< "show State:/Users/ConsoleUser" | /usr/bin/awk '/Name :/ && ! /loginwindow/ { print $3 }' )
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost write com.apple.Bluetooth PrefKeyServicesEnabled -bool false
```

CCI: CCI-000213

CCI: CCI-000381

Group ID (Vulid): V-268519
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268519r1034497_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002120
Rule Title: The macOS system must disable AppleID and internet Account Modification.

Vulnerability Discussion: The system must disable Account Modification.

Account Modification includes adding or modifying internet accounts in Apple Mail, Calendar, or 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.

CCI: CCI-000381

Group ID (Vulid): V-268521
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268521r1034503_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002140
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-268522
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268522r1034506_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002150
Rule Title: The macOS system must disable iCloud Desktop and Document folder sync.

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-268523
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268523r1034509_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002160
Rule Title: The macOS system must disable iCloud Game Center.

Vulnerability Discussion: This works only with supervised devices (mobile device management [MDM]) and allows to disable Apple Game Center. The rationale is that 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-268524
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268524r1034512_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002170
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-268525
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268525r1131237_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002180
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 must 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('DisableFMMiCloudSetting'))
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" and "com.apple.icloud.managed" configuration profiles.

CCI: CCI-000381

Group ID (Vulid): V-268526
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268526r1034518_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002200
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-268527
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268527r1034521_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002210
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-268528
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268528r1034524_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002220
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 Only 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 Only Dictation by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268529
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268529r1034527_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002230
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-268530
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268530r1034530_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002240
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-268531
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268531r1034533_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002250
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-268532
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268532r1034536_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002260
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-268533
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268533r1034539_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002270
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.

Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable 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-272477
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-272477r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-002271
Rule Title: The macOS system must disable iPhone Mirroring.

Vulnerability Discussion: iPhone Mirroring must be disabled to prevent file transfers to or from unauthorized devices.

Disabling iPhone Mirroring also prevents potentially unauthorized applications from appearing as if they are installed on the Mac.

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 iPhone Mirroring with the following command:

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

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

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

CCI: CCI-000213

CCI: CCI-000381

CCI: CCI-001443

Group ID (Vulid): V-268534
Group Title: SRG-OS-000403-GPOS-00182
Rule ID: SV-268534r1268247_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003001
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.

Satisfies: SRG-OS-000403-GPOS-00182, SRG-OS-000775-GPOS-00230

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

CCI: CCI-004909

Group ID (Vulid): V-268535
Group Title: SRG-OS-000071-GPOS-00039
Rule ID: SV-268535r1034545_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003007
Rule Title: The macOS system must require that 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 states that complexity rules should be organizationally defined. The values defined are based on common complexity values, but each organization may define its own password complexity rules.

Check Content:
Verify the macOS system is configured to require that 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 that passwords contain a minimum of one numeric character by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

Group ID (Vulid): V-268536
Group Title: SRG-OS-000076-GPOS-00044
Rule ID: SV-268536r1268211_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003008
Rule Title: The macOS system must restrict maximum password lifetime to 180 days.

Vulnerability Discussion: The macOS must be configured to enforce a maximum password lifetime limit of at least 180 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 states that complexity rules should be organizationally defined. The values defined are based on common complexity values, but each organization may define its own password complexity rules.

Check Content:
Verify the macOS system is configured to restrict maximum password lifetime to 180 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 "180" or less, this is a finding.

Fix Text: Configure the macOS system to restrict maximum password lifetime to 180 days by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

Group ID (Vulid): V-268537

Group Title: SRG-OS-000078-GPOS-00046
Rule ID: SV-268537r1034551_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003010
Rule Title: The macOS system must require a minimum password length of 14 characters.

Vulnerability Discussion: The macOS must be configured to require that 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 states that complexity rules should be organizationally defined. The values defined are based on common complexity values, but each 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

Group ID (Vulid): V-268538
Group Title: SRG-OS-000266-GPOS-00101
Rule ID: SV-268538r1131239_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003011
Rule Title: The macOS system must require that passwords contain a minimum of one special character.

Vulnerability Discussion: The macOS must be configured to require that at least one special character be used when a password is created.

Special characters are 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 states that complexity rules must be organizationally defined. The values defined are based on common complexity values, but each 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 -n +2 | /usr/bin/xmllint --xpath
"//string[contains(text(), \"policyAttributePassword matches '(.*[^a-zA-Z0-9].*){\")]" - 2>/dev/null | /usr/bin/awk
-F"{|}" '{if ($2 >= 1) {print "true"} else {print "false"}}'
```

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

Fix Text: Configure the macOS system to require that passwords contain a minimum of one special character by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

CCI: CCI-004066

Group ID (Vulid): V-268539
Group Title: SRG-OS-000079-GPOS-00047
Rule ID: SV-268539r1034557_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003012
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-268540
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-268540r1268251_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003013
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 the 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. Users must 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-268541
Group Title: SRG-OS-000079-GPOS-00047
Rule ID: SV-268541r1131242_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003014
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 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:

HINT=$(/usr/bin/dscl . -list /Users hint | /usr/bin/awk '{ print $2 }')

if [-z "$HINT"]; then
echo "PASS"
else
echo "FAIL"

```
fi
```

If the result is not "PASS", 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-268542
Group Title: SRG-OS-000067-GPOS-00035
Rule ID: SV-268542r1034566_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003020
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 login, authorization, and unlocking the screen saver.

CAUTION: enforceSmartCard will apply to the whole system. No users will be able to log in 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" 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, SRG-OS-000705-GPOS-00150

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-004047

Group ID (Vulid): V-268543
Group Title: SRG-OS-000068-GPOS-00036
Rule ID: SV-268543r1034569_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003030
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 login, 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

Group ID (Vulid): V-268544
Group Title: SRG-OS-000105-GPOS-00052
Rule ID: SV-268544r1268228_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003050
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, SRG-OS-000705-GPOS-00150

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

Group ID (Vulid): V-268545
Group Title: SRG-OS-000105-GPOS-00052
Rule ID: SV-268545r1268228_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003051
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, SRG-OS-000705-GPOS-00150

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

Group ID (Vulid): V-268546
Group Title: SRG-OS-000105-GPOS-00052
Rule ID: SV-268546r1268228_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003052
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, SRG-OS-000705-GPOS-00150

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

Group ID (Vulid): V-268547
Group Title: SRG-OS-000069-GPOS-00037
Rule ID: SV-268547r1034581_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003060
Rule Title: The macOS system must require that passwords contain a minimum of one lowercase character and one uppercase character.

Vulnerability Discussion: The macOS must be configured to require that 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 states that complexity rules should be organizationally defined. The values defined are based on common complexity values, but each organization may define its own password complexity rules.

NOTE: The configuration profile generated must be installed from a Mobile Device Management (MDM) server.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038, SRG-OS-000730-GPOS-00190

Check Content:
Verify the macOS system is configured to require that 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-004065

Group ID (Vulid): V-268548
Group Title: SRG-OS-000075-GPOS-00043
Rule ID: SV-268548r1131244_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003070
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 states that complexity rules must be organizationally defined. The values defined are based on common complexity values, but each 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.

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 < 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

Group ID (Vulid): V-268549
Group Title: SRG-OS-000118-GPOS-00060
Rule ID: SV-268549r1131246_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-003080
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 employing unused accounts to gain access to the system while avoiding detection.

Satisfies: SRG-OS-000118-GPOS-00060, SRG-OS-000590-GPOS-00110

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.

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 > 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

Group ID (Vulid): V-268550
Group Title: SRG-OS-000205-GPOS-00083
Rule ID: SV-268550r1034590_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-004001
Rule Title: The macOS system must configure Apple System Log (ASL) files owned by root and group to wheel.

Vulnerability Discussion: The Apple System Logs must be owned by root.

ASLs contain sensitive data about the system and users. Setting ASL files to be readable and writable only by system administrators mitigates the risk.

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

Check Content:
Verify the macOS system is configured with ASL 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 ASL 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-268551
Group Title: SRG-OS-000205-GPOS-00083
Rule ID: SV-268551r1034593_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-004002
Rule Title: The macOS system must configure Apple System Log (ASL) files to mode 640 or less permissive.

Vulnerability Discussion: The Apple System Logs must be configured to be writable by root and readable only by the root user and group wheel. To achieve this, ASL 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 ASL 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 ASL 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":" '!/640/{print $2}')

CCI: CCI-001312

CCI: CCI-001314

Group ID (Vulid): V-274881
Group Title: SRG-OS-000373-GPOS-00156
Rule ID: SV-274881r1099904_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-004022
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_timout 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

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-002038

CCI: CCI-004895

Group ID (Vulid): V-268552
Group Title: SRG-OS-000205-GPOS-00083
Rule ID: SV-268552r1034596_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-004030
Rule Title: The macOS system must configure system log files 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. Setting log files to be readable and writable only by system administrators mitigates the risk.

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-268553
Group Title: SRG-OS-000205-GPOS-00083
Rule ID: SV-268553r1034599_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-004040
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-268554
Group Title: SRG-OS-000341-GPOS-00132
Rule ID: SV-268554r1034602_rule
Severity: CAT III
Rule Version (STIG-ID): APPL-15-004050
Rule Title: The macOS system must configure install.log retention to 365.

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

Proper audit storage capacity is crucial to ensuring the ongoing logging of critical events.

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 the extra files"} else if (max == "True") { print "all_max setting is configured, must be removed" } if (ttl != "True") { print "TTL not configured" } 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 multiple configuration files in /etc/asl are set to process the file /var/log/install.log, these files must be manually removed.

CCI: CCI-001849

Group ID (Vulid): V-274880
Group Title: SRG-OS-000373-GPOS-00156
Rule ID: SV-274880r1099901_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-004060
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-002038

CCI: CCI-004895

Group ID (Vulid): V-268555
Group Title: SRG-OS-000051-GPOS-00024
Rule ID: SV-268555r1034605_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-005001
Rule Title: The macOS system must ensure System Integrity Protection is enabled.

Vulnerability Discussion: System Integrity Protection 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: System Integrity Protection 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-000138-GPOS-00069, 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, launching "Terminal" from the "Utilities" menu, and running 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-001876

CCI: CCI-001090

CCI: CCI-001493

CCI: CCI-001494

CCI: CCI-001495

CCI: CCI-001499

CCI: CCI-001496

CCI: CCI-001878

Group ID (Vulid): V-268556
Group Title: SRG-OS-000185-GPOS-00079
Rule ID: SV-268556r1131248_rule
Severity: CAT I
Rule Version (STIG-ID): APPL-15-005020
Rule Title: The macOS system must enforce FileVault.

Vulnerability Discussion: 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: Refer to the FileVault supplemental to implement this rule. Configure the macOS system to enforce FileVault by installing the "com.apple.MCX" configuration profile.

CCI: CCI-001199

CCI: CCI-002475

CCI: CCI-002476

Group ID (Vulid): V-268557
Group Title: SRG-OS-000480-GPOS-00232
Rule ID: SV-268557r1034611_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005050
Rule Title: The macOS system must enable macOS 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:

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

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

Fix Text: Configure the macOS system to enable the Application Firewall by installing the "com.apple.security.firewall" configuration profile.

CCI: CCI-000366

Group ID (Vulid): V-268558
Group Title: SRG-OS-000104-GPOS-00051
Rule ID: SV-268558r1034614_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005052
Rule Title: The macOS system must configure the 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 login window by installing the "com.apple.loginwindow" configuration profile.

CCI: CCI-000764

Group ID (Vulid): V-268559
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268559r1034617_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005054
Rule Title: The macOS system must disable the 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 the risk of individuals electing to enable TouchID to override organizationwide settings.

Check Content:
Verify the macOS system is configured to disable the 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 the TouchID prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268560
Group Title: SRG-OS-000095-GPOS-00049

Rule ID: SV-268560r1034620_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005055
Rule Title: The macOS system must disable the Screen Time prompt during Setup Assistant.

Vulnerability Discussion: The prompt for Screen Time setup during Setup Assistant must be disabled.

Enabling any service increases the attack surface for an intruder. By disabling unnecessary services, the attack surface is minimized.

Check Content:
Verify the macOS system is configured to disable the 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 the Screen Time prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268561
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268561r1034623_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005056
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 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 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-268562
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268562r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005058
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

CCI: CCI-001443

Group ID (Vulid): V-268563
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268563r1034629_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005060
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.

CCI: CCI-000381

Group ID (Vulid): V-268564
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268564r1034632_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005061
Rule Title: The macOS system must disable Erase Content and Settings.

Vulnerability Discussion: Erase Content and Settings must be disabled.

Without disabling the Erase Content and Settings configuration, forensics data could be lost if this feature is activated on a compromised system.

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-268565
Group Title: SRG-OS-000080-GPOS-00048
Rule ID: SV-268565r1268226_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005070
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/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "AuthenticatedRootVolumeEnabled = 1;"

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-268566
Group Title: SRG-OS-000362-GPOS-00149
Rule ID: SV-268566r1131250_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005080
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 regular users without 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.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 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

Group ID (Vulid): V-268567
Group Title: SRG-OS-000378-GPOS-00163
Rule ID: SV-268567r1131252_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005090
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.
====

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Satisfies: SRG-OS-000378-GPOS-00163, SRG-OS-000690-GPOS-00140

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-268568
Group Title: SRG-OS-000445-GPOS-00199
Rule ID: SV-268568r1034644_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005100
Rule Title: The macOS system must ensure Secure Boot level is 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 a 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 is 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 is set to "full" by booting into Recovery Mode and enabling Full Secure Boot.

CCI: CCI-002696

CCI: CCI-002699

CCI: CCI-002702

Group ID (Vulid): V-268569
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-268569r1268251_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005110
Rule Title: The macOS system must enforce enrollment in Mobile Device Management (MDM).

Vulnerability Discussion: Users must enroll their Mac in 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.
* 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 the system is enrolled via UAMDM.

CCI: CCI-000366

Group ID (Vulid): V-268570
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-268570r1268251_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005120
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-268571
Group Title: SRG-OS-000480-GPOS-00227
Rule ID: SV-268571r1268251_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005130
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 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.

CCI: CCI-000366

Group ID (Vulid): V-268572
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268572r1034656_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005140
Rule Title: The macOS system must disable Genmoji.

Vulnerability Discussion: Apple Intelligence features that use off-device Artificial Intelligence (AI) must be disabled.

Use of off-device AI poses a data loss risk.

Check Content:
Verify the macOS system is configured to disable Genmoji with the following command:

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

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

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

CCI: CCI-000381

Group ID (Vulid): V-268573
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268573r1034659_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005150
Rule Title: The macOS system must disable Apple Intelligence Image Generation.

Vulnerability Discussion: Apple Intelligence features that use off-device artificial intelligence must be disabled.

Use of off-device AI poses a data loss risk.

Check Content:
Verify the macOS system is configured to disable Apple Intelligence Image Generation with the following command:

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

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

Fix Text: Configure the macOS system to disable Apple Intelligence Image Generation by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268574
Group Title: SRG-OS-000095-GPOS-00049
Rule ID: SV-268574r1034662_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-005160
Rule Title: The macOS system must disable Apple Intelligence Writing Tools.

Vulnerability Discussion: Apple Intelligence features that use off device Artificial Intelligence must be disabled.

Use of off-device AI poses a data loss risk.

Check Content:

Verify the macOS system is configured to disable Apple Intelligence Writing Tools with the following command:

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

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

Fix Text: Configure the macOS system to disable Apple Intelligence Writing Tools by installing the "com.apple.applicationaccess" configuration profile.

CCI: CCI-000381

Group ID (Vulid): V-268575
Group Title: SRG-OS-000439-GPOS-00195
Rule ID: SV-268575r1149426_rule
Severity: CAT II
Rule Version (STIG-ID): APPL-15-999999
Rule Title: The macOS system must install security-relevant software updates within 30 days unless the time period is directed by an authoritative source (e.g., IAVM, CTOs, DTMs, STIGs).

Vulnerability Discussion: Security flaws with operating systems are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Check Content:
Verify security-relevant software updates are installed on the operating system within 30 days unless the time period is directed by an authoritative source (e.g., IAVM, CTOs, DTMs, STIGs).

Click the Apple icon on the menu at the top left corner of the screen.
Select the "About This Mac" option.
Select the "More Info..." button.
Under the macOS section, there are details about the update version.
Compare this to the latest available macOS update version.

If the installed updates are not the latest and the latest updates have been available for 30 days or more, this is a finding.

Fix Text: Install the latest updates within 30 days unless the time period is directed by an authoritative source (e.g., IAVM, CTOs, DTMs, STIGs).

CCI: CCI-002605