CIS Apple macOS 15 (Sequoia) STIG Benchmark

v1.0.0 – 07-02-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Internal Only - General

Table of Contents

Internal Only - General

Internal Only - General

Internal Only - General

Internal Only - General

Overview

Target Technology Details

Apple macOS 15 (Sequoia) Secure Technical Implementation Guide (STIG)
Version: 1 Release: 4 Benchmark
Date: 02 Jul 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Apple macOS 15 (Sequoia) and are looking to comply with the STIG guidance

Internal Only - General

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Internal Only - General

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Internal Only - General

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Internal Only - General

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Apple macOS 15 (Sequoia)

Internal Only - General

Recommendations

1 STIG RULES

Apple macOS 15.0

Apple macOS 15 (Sequoia) Secure Technical Implementation Guide (STIG)

Version: 1 Release: 4 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

Internal Only - General

1.1 APPL-15-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268420
RULE ID: SV-268420r1034200
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

Internal Only - General

1.2 APPL-15-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce screen saver password.

```
GROUP ID: V-268421
RULE ID: SV-268421r1034203
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to prompt users to enter a password to unlock the screen saver by installing the "com.apple.screensaver" configuration profile.

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

Internal Only - General

1.3 APPL-15-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268422
RULE ID: SV-268422r1034206
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

Internal Only - General

1.4 APPL-15-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268423
RULE ID: SV-268423r1034209
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

Internal Only - General

1.5 APPL-15-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable hot corners.

```
GROUP ID: V-268424
RULE ID: SV-268424r1034212
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.6 APPL-15-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268425
RULE ID: SV-268425r1034215
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.7 APPL-15-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268426
RULE ID: SV-268426r1034218
```

Rationale:

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.

Internal Only - General

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

Audit:

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 "policyCategoryAuthentication".
In the array that follows, there should be a section that contains a check 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.

Internal Only - General

Remediation:

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 <
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
```

Additional Information:

CCI-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53 Revision 5::AC-2 (2)

CCI-001682 Automatically remove or disable emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 Revision 5::AC-2 (2)
- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)

Internal Only - General

1.8 APPL-15-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must limit consecutive failed login attempts to three.

```
GROUP ID: V-268428
RULE ID: SV-268428r1034224
```

Rationale:

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

Audit:

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"}}'
```

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

Remediation:

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

Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.9 APPL-15-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce time synchronization.

```
GROUP ID: V-268427
RULE ID: SV-268427r1038944
```

Rationale:

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

Audit:

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.

Remediation:

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

Internal Only - General

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

Internal Only - General

1.10 APPL-15-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must display a policy banner at remote login.

```
GROUP ID: V-268429
RULE ID: SV-268429r1034227
```

Rationale:

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

Internal Only - General

Audit:

Verify the macOS system is configured to display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system.
Verify the operating system has the correct text listed in the "/etc/banner" file with the following command:

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

The command must return the following text:

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

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

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

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

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

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

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

If the operating system does not display a login banner before granting remote access or the banner does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.
If the text in the "/etc/banner" file does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

Remediation:

Configure the macOS system to display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system by creating a text file containing the required DOD text.
Name the file "banner" and place it in "/etc/".

Internal Only - General

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

Internal Only - General

1.11 APPL-15-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce SSH to display a policy banner.

```
GROUP ID: V-269093
RULE ID: SV-269093r1034754
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

Internal Only - General

1.12 APPL-15-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268431
RULE ID: SV-268431r1034233
```

Rationale:

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

Internal Only - General

Audit:

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 permissions for "PolicyBanner.rtfd" are not "644", this is a finding.
The banner text of the document must read:

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

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

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

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

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

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

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

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

Internal Only - General

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

Internal Only - General

1.13 APPL-15-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit log files to not contain access control lists (ACLs).

```
GROUP ID: V-268432
RULE ID: SV-268432r1034236
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.14 APPL-15-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure the audit log folder to not contain access control lists (ACLs).

```
GROUP ID: V-268433
RULE ID: SV-268433r1034239
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.15 APPL-15-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable FileVault automatic login.

```
GROUP ID: V-268434
RULE ID: SV-268434r1034242
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.16 APPL-15-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure SSHD ClientAliveInterval to 900.

```
GROUP ID: V-268435
RULE ID: SV-268435r1034245
```

Rationale:

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 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.

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

Internal Only - General

1.17 APPL-15-000052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure SSHD ClientAliveCountMax to 1.

```
GROUP ID: V-268436
RULE ID: SV-268436r1034780
```

Rationale:

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.

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

Internal Only - General

1.18 APPL-15-000053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must set login grace time to 30.

```
GROUP ID: V-268437
RULE ID: SV-268437r1034251
```

Rationale:

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.

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

Internal Only - General

1.19 APPL-15-000054 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-268438
RULE ID: SV-268438r1034254
```

Rationale:

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

Internal Only - General

Audit:

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.

Remediation:

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

```
/bin/ln -fs /etc/ssh/crypto/fips.conf /etc/ssh/crypto.conf
```


Internal Only - General

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

Internal Only - General

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

Internal Only - General

1.20 APPL-15-000057 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-268439
RULE ID: SV-268439r1034803
```

Rationale:

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

Internal Only - General

Audit:

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.

Internal Only - General

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

Internal Only - General

1.21 APPL-15-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268440
RULE ID: SV-268440r1034260
```

Rationale:

The macOS system must be configured to enforce a lockout time period 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

Audit:

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

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

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

Remediation:

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

Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.22 APPL-15-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce screen saver timeout.

```
GROUP ID: V-268441
RULE ID: SV-268441r1034263
```

Rationale:

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.

Audit:

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.

Remediation:

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

Internal Only - General

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

Internal Only - General

1.23 APPL-15-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable login to other users' active and locked sessions.

```
GROUP ID: V-268442
RULE ID: SV-268442r1034266
```

Rationale:

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

macOS has a privilege that can be granted to any user that will allow that user to unlock active 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

Audit:

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.

Remediation:

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"
```


Internal Only - General

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

Internal Only - General

1.24 APPL-15-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable root login.

```
GROUP ID: V-268443
RULE ID: SV-268443r1034269
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

Internal Only - General

1.25 APPL-15-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure the SSH ServerAliveInterval to 900.

```
GROUP ID: V-268444
RULE ID: SV-268444r1034800
```

Rationale:

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.

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

Internal Only - General

1.26 APPL-15-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure SSHD channel timeout to 900.

```
GROUP ID: V-268445
RULE ID: SV-268445r1034275
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

Internal Only - General

1.27 APPL-15-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268446
RULE ID: SV-268446r1034278
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

Internal Only - General

1.28 APPL-15-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268447
RULE ID: SV-268447r1034805
```

Rationale:

SSH must be configured with an Active Server Alive Maximum Count set to 0. Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. 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.

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

Internal Only - General

1.29 APPL-15-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268448
RULE ID: SV-268448r1034284
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

Internal Only - General

1.30 APPL-15-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268449
RULE ID: SV-268449r1038944
```

Rationale:

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

Audit:

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 DOD network, this is a finding.

Remediation:

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

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

Internal Only - General

1.31 APPL-15-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enable the time synchronization daemon.

```
GROUP ID: V-268450
RULE ID: SV-268450r1038944
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

Internal Only - General

1.32 APPL-15-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure sudo to log events.

```
GROUP ID: V-268451
RULE ID: SV-268451r1034293
```

Rationale:

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.

Audit:

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.

Remediation:

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

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i '' '/Defaults
\!log_allowed/d' '{}' \;
/bin/echo "Defaults log_allowed" >> /etc/sudoers.d/mscp
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

1.33 APPL-15-001001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268452
RULE ID: SV-268452r1034296
```

Rationale:

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

Audit:

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

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

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

Internal Only - General

Remediation:

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.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)

Internal Only - General

- NIST SP 800-53 Revision 5::AC-6 (9)

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

1.34 APPL-15-001002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must be configured to audit all login and logout events.

```
GROUP ID: V-268453
RULE ID: SV-268453r1034299
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.35 APPL-15-001003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enable security auditing.

```
GROUP ID: V-268454
RULE ID: SV-268454r1034302
```

Rationale:

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

Internal Only - General

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)

Internal Only - General

- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000159 Use internal system clocks to generate time stamps for audit records.

- NIST SP 800-53::AU-8
- NIST SP 800-53A::AU-8.1
- NIST SP 800-53 Revision 4::AU-8 a
- NIST SP 800-53 Revision 5::AU-8 a

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 f

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4::AU-12 (3)
- NIST SP 800-53 Revision 5::AU-12 (3)

Internal Only - General

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5::MA-3 (5)

Internal Only - General

1.36 APPL-15-001010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must be configured to shut down upon audit failure.

```
GROUP ID: V-268455
RULE ID: SV-268455r1038966
```

Rationale:

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.

Audit:

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.

Remediation:

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
```

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

Internal Only - General

1.37 APPL-15-001012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit log files to be owned by root.

```
GROUP ID: V-268456
RULE ID: SV-268456r1034308
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.38 APPL-15-001013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit log folders to be owned by root.

```
GROUP ID: V-268457
RULE ID: SV-268457r1034311
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.39 APPL-15-001014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure the audit log files group to wheel.

```
GROUP ID: V-268458
RULE ID: SV-268458r1034314
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.40 APPL-15-001015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure the audit log folders group to wheel.

```
GROUP ID: V-268459
RULE ID: SV-268459r1034317
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.41 APPL-15-001016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268460
RULE ID: SV-268460r1034320
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.42 APPL-15-001017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268461
RULE ID: SV-268461r1034323
```

Rationale:

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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.43 APPL-15-001020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268462
RULE ID: SV-268462r1034326
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.44 APPL-15-001021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268463
RULE ID: SV-268463r1034329
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.45 APPL-15-001022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268464
RULE ID: SV-268464r1034332
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.46 APPL-15-001023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268465
RULE ID: SV-268465r1034335
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.47 APPL-15-001024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-269094
RULE ID: SV-269094r1034757
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

1.48 APPL-15-001029 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The macOS system must configure audit retention to seven days.

```
GROUP ID: V-268467
RULE ID: SV-268467r1034341
```

Rationale:

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.

Audit:

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.

Remediation:

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
```

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

Internal Only - General

1.49 APPL-15-001030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit capacity warning.

```
GROUP ID: V-268468
RULE ID: SV-268468r1034344
```

Rationale:

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

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

Internal Only - General

1.50 APPL-15-001031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit failure notification.

```
GROUP ID: V-268469
RULE ID: SV-268469r1038966
```

Rationale:

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

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

Internal Only - General

1.51 APPL-15-001044 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must be configured to audit all authorization and authentication events.

```
GROUP ID: V-268470
RULE ID: SV-268470r1034350
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

1.52 APPL-15-001060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268471
RULE ID: SV-268471r1034353
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5::IA-5 (2) (b) (2)

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

Internal Only - General

1.53 APPL-15-001100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable root login for SSH.

```
GROUP ID: V-268472
RULE ID: SV-268472r1034356
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

Internal Only - General

1.54 APPL-15-001110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit_control group to wheel.

```
GROUP ID: V-268473
RULE ID: SV-268473r1034359
```

Rationale:

/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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.55 APPL-15-001120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit_control owner to root.

```
GROUP ID: V-268474
RULE ID: SV-268474r1034362
```

Rationale:

/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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.56 APPL-15-001130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit_control owner to mode 440 or less permissive.

```
GROUP ID: V-268475
RULE ID: SV-268475r1034365
```

Rationale:

/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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.57 APPL-15-001140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure audit_control to not contain access control lists (ACLs).

```
GROUP ID: V-269095
RULE ID: SV-269095r1034760
```

Rationale:

/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

Audit:

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.

Remediation:

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

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


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

Internal Only - General

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.58 APPL-15-001150 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must disable password authentication for SSH.

```
GROUP ID: V-268477
RULE ID: SV-268477r1034371
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

Internal Only - General

1.59 APPL-15-002001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Server Message Block (SMB) sharing.

```
GROUP ID: V-268478
RULE ID: SV-268478r1034374
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.60 APPL-15-002003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Network File System (NFS) service.

```
GROUP ID: V-268479
RULE ID: SV-268479r1034377
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.61 APPL-15-002004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Location Services.

```
GROUP ID: V-268480
RULE ID: SV-268480r1034380
```

Rationale:

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.

Audit:

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.

Remediation:

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
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.62 APPL-15-002005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Bonjour multicast.

```
GROUP ID: V-268481
RULE ID: SV-268481r1034383
```

Rationale:

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

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.63 APPL-15-002006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Unix-to-Unix Copy Protocol (UUCP) service.

```
GROUP ID: V-268482
RULE ID: SV-268482r1034386
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.64 APPL-15-002007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Internet Sharing.

```
GROUP ID: V-268483
RULE ID: SV-268483r1034389
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.65 APPL-15-002008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268484
RULE ID: SV-268484r1034392
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.66 APPL-15-002009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable AirDrop.

```
GROUP ID: V-268485
RULE ID: SV-268485r1034395
```

Rationale:

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

Audit:

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.

Remediation:

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

Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

Internal Only - General

1.67 APPL-15-002010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable FaceTime.app.

```
GROUP ID: V-268486
RULE ID: SV-268486r1034398
```

Rationale:

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.yaml#L67-L70). Using these controls may not work as expected. Third-party software may be required to fulfill the compliance requirements.

Audit:

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.applicationac
cess.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.

Internal Only - General

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.68 APPL-15-002012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the iCloud Calendar services.

```
GROUP ID: V-268487
RULE ID: SV-268487r1034401
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.69 APPL-15-002013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Reminders.

```
GROUP ID: V-268488
RULE ID: SV-268488r1034404
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.70 APPL-15-002014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Address Book.

```
GROUP ID: V-268489
RULE ID: SV-268489r1034407
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.71 APPL-15-002015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Mail.

```
GROUP ID: V-268490
RULE ID: SV-268490r1034410
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.72 APPL-15-002016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Notes.

```
GROUP ID: V-268491
RULE ID: SV-268491r1034413
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.73 APPL-15-002017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the camera.

```
GROUP ID: V-268492
RULE ID: SV-268492r1034416
```

Rationale:

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.

Audit:

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.

Internal Only - General

Remediation:

Configure the macOS system to disable the camera by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.74 APPL-15-002020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Siri.

```
GROUP ID: V-268493
RULE ID: SV-268493r1034419
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.75 APPL-15-002021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268494
RULE ID: SV-268494r1034422
```

Rationale:

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

Audit:

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.

Remediation:

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

Internal Only - General

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.76 APPL-15-002022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Remote Apple Events.

```
GROUP ID: V-268495
RULE ID: SV-268495r1034425
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

Internal Only - General

1.77 APPL-15-002023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable sending audio recordings and transcripts to Apple.

```
GROUP ID: V-269096
RULE ID: SV-269096r1034785
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.78 APPL-15-002024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable sending search data from Spotlight to Apple.

```
GROUP ID: V-269566
RULE ID: SV-269566r1034793
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.79 APPL-15-002035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-268496
RULE ID: SV-268496r1034428
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.80 APPL-15-002036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Privacy Setup services during Setup Assistant.

```
GROUP ID: V-268497
RULE ID: SV-268497r1034431
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Privacy Setup services during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.81 APPL-15-002037 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud storage setup during Setup Assistant.

```
GROUP ID: V-268498
RULE ID: SV-268498r1034434
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud storage setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.82 APPL-15-002038 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must disable Trivial File Transfer Protocol (TFTP) service.

```
GROUP ID: V-268499
RULE ID: SV-268499r1034437
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)
- NIST SP 800-53 Revision 5::IA-5 (1) (c)

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.83 APPL-15-002039 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Siri Setup during Setup Assistant.

```
GROUP ID: V-268500
RULE ID: SV-268500r1034440
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Siri Setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.84 APPL-15-002040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Keychain Sync.

```
GROUP ID: V-268501
RULE ID: SV-268501r1034443
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud Keychain Sync by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.85 APPL-15-002041 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Document Sync.

```
GROUP ID: V-268502
RULE ID: SV-268502r1034446
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud Document Sync by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.86 APPL-15-002042 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Bookmarks.

```
GROUP ID: V-268503
RULE ID: SV-268503r1034449
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud Bookmarks by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.87 APPL-15-002043 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Photo Library.

```
GROUP ID: V-268504
RULE ID: SV-268504r1034452
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable the iCloud Photo Library by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.88 APPL-15-002050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Screen Sharing and Apple Remote Desktop.

```
GROUP ID: V-268505
RULE ID: SV-268505r1034455
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.89 APPL-15-002052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the System Settings pane for Wallet and Apple Pay.

```
GROUP ID: V-268506
RULE ID: SV-268506r1034458
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable the System Settings pane for Wallet and Apple Pay by installing the "com.apple.systempreferences" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.90 APPL-15-002053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the system settings pane for Siri.

```
GROUP ID: V-268507
RULE ID: SV-268507r1034461
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable the system settings pane for Siri by installing the "com.apple.systempreferences" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.91 APPL-15-002060 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must apply gatekeeper settings to block applications from unidentified developers.

```
GROUP ID: V-268508
RULE ID: SV-268508r1034464
```

Rationale:

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.

Audit:

Verify the macOS system is configured to apply gatekeeper settings to block applications from unidentified developers with the following command:

```
/usr/sbin/spctl --status --verbose | /usr/bin/grep -c "developer id enabled"
```

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

Remediation:

Configure the macOS system to apply gatekeeper settings to block applications from unidentified developers with the following command:

```
/usr/sbin/spctl --global-enable; /usr/sbin/spctl --enable
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

Internal Only - General

1.92 APPL-15-002062 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must disable Bluetooth when no approved device is connected.

```
GROUP ID: V-268509
RULE ID: SV-268509r1034467
```

Rationale:

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

Audit:

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.

Remediation:

Configure the macOS system to disable Bluetooth by installing the "com.apple.MCXBluetooth" configuration profile.

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

Internal Only - General

1.93 APPL-15-002063 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the guest account.

```
GROUP ID: V-268510
RULE ID: SV-268510r1034470
```

Rationale:

Guest access must be disabled.

Turning off guest access prevents anonymous users from accessing files.

Audit:

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.

Remediation:

Configure the macOS system to disable the guest account by installing the "com.apple.MCX" configuration profile.

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

Internal Only - General

1.94 APPL-15-002064 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must enable gatekeeper.

```
GROUP ID: V-268511
RULE ID: SV-268511r1034473
```

Rationale:

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 that the application has not been modified by a malicious third party.

Administrator users will still have the option to override these settings on a case-by-case basis.

Audit:

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

```
/usr/sbin/spctl --status | /usr/bin/grep -c "assessments enabled"
```

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

Remediation:

Configure the macOS system to enable gatekeeper with the following command:

```
/usr/sbin/spctl --global-enable
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

Internal Only - General

1.95 APPL-15-002066 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must disable unattended or automatic login to the system.

```
GROUP ID: V-268512
RULE ID: SV-268512r1034476
```

Rationale:

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

Audit:

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.

Remediation:

Configure the macOS system to disable unattended or automatic login to the system by installing the "com.apple.loginwindow" configuration profile.

Internal Only - General

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.96 APPL-15-002068 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must secure users' home folders.

```
GROUP ID: V-268513
RULE ID: SV-268513r1034479
```

Rationale:

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

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.97 APPL-15-002069 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must require an administrator password to modify systemwide preferences.

```
GROUP ID: V-268514
RULE ID: SV-268514r1034482
```

Rationale:

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.

Internal Only - General

Audit:

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.

Internal Only - General

Remediation:

Configure the macOS system to require administrator privileges to modify systemwide settings with the following command:

Internal Only - General

```
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" <
```


Internal Only - General

```
"/tmp/$section.plist"
done
```


Internal Only - General

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

Internal Only - General

1.98 APPL-15-002080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Airplay Receiver.

```
GROUP ID: V-268515
RULE ID: SV-268515r1034485
```

Rationale:

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

Audit:

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.

Remediation:

Configure the macOS system to disable Airplay Receiver by installing the "com.apple.applicationaccess" configuration profile.

Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

Internal Only - General

1.99 APPL-15-002090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable TouchID for unlocking the device.

```
GROUP ID: V-268516
RULE ID: SV-268516r1034488
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable TouchID for unlocking the device by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

Internal Only - General

1.100 APPL-15-002100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Media Sharing.

```
GROUP ID: V-268517
RULE ID: SV-268517r1034491
```

Rationale:

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.

Audit:

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

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

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

Remediation:

Configure the macOS system to disable Media Sharing by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.101 APPL-15-002110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Bluetooth Sharing.

```
GROUP ID: V-268518
RULE ID: SV-268518r1034494
```

Rationale:

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

Audit:

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

```
/usr/bin/defaults -currentHost read com.apple.Bluetooth
PrefKeyServicesEnabled
```

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

Remediation:

Configure the macOS system to disable Bluetooth sharing with the following command:

```
/usr/bin/defaults -currentHost write com.apple.Bluetooth
PrefKeyServicesEnabled -bool false
```


Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.102 APPL-15-002120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable AppleID and internet Account Modification.

```
GROUP ID: V-268519
RULE ID: SV-268519r1034497
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Account Modification by installing the "com.apple.applicationaccess" configuration profile.

Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.103 APPL-15-002130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable CD/DVD Sharing.

```
GROUP ID: V-268520
RULE ID: SV-268520r1034500
```

Rationale:

CD/DVD Sharing must be disabled.

Audit:

Verify the macOS system is configured to disable CD/DVD Sharing with the following command:

```
/usr/bin/pgrep -q ODSAgent; /bin/echo $?
```

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

Remediation:

Configure the macOS system to disable CD/DVD Sharing with the following command:

```
/bin/launchctl unload /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.104 APPL-15-002140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Content Caching service.

```
GROUP ID: V-268521
RULE ID: SV-268521r1034503
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Content Caching service by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.105 APPL-15-002150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Desktop and Document folder sync.

```
GROUP ID: V-268522
RULE ID: SV-268522r1034506
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud Desktop and Document folder synchronization by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.106 APPL-15-002160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Game Center.

```
GROUP ID: V-268523
RULE ID: SV-268523r1034509
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud Game Center by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.107 APPL-15-002170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iCloud Private Relay.

```
GROUP ID: V-268524
RULE ID: SV-268524r1034512
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable the iCloud Private Relay by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.108 APPL-15-002180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Find My service.

```
GROUP ID: V-268525
RULE ID: SV-268525r1034515
```

Rationale:

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.

Audit:

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($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationac
cess')\
.objectForKey('allowFindMyDevice'))
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationac
cess')\
.objectForKey('allowFindMyFriends'))
  let pref3 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.icloud.manage
d')\
.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.

Internal Only - General

Remediation:

Configure the macOS system to disable Find My service by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.109 APPL-15-002200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Personalized Advertising.

```
GROUP ID: V-268526
RULE ID: SV-268526r1034518
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Personalized Advertising by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.110 APPL-15-002210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable sending Siri and Dictation information to Apple.

```
GROUP ID: V-268527
RULE ID: SV-268527r1034521
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable sending Siri and Dictation information to Apple by installing the "com.apple.assistant.support" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.111 APPL-15-002220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce On Device Dictation.

```
GROUP ID: V-268528
RULE ID: SV-268528r1034524
```

Rationale:

Dictation must be restricted to On Device Only to prevent potential data exfiltration.

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

Audit:

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.

Remediation:

Configure the macOS system to enforce On Device Only Dictation by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.112 APPL-15-002230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Dictation.

```
GROUP ID: V-268529
RULE ID: SV-268529r1034527
```

Rationale:

Dictation must be disabled on Intel-based Macs as the feature On Device Dictation is only available on Apple Silicon devices.

Audit:

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.

Remediation:

Configure the macOS system to disable Dictation by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.113 APPL-15-002240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Printer Sharing.

```
GROUP ID: V-268530
RULE ID: SV-268530r1034530
```

Rationale:

Printer Sharing must be disabled.

Audit:

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.

Remediation:

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
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.114 APPL-15-002250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Remote Management.

```
GROUP ID: V-268531
RULE ID: SV-268531r1034533
```

Rationale:

Remote Management must be disabled.

Audit:

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.

Remediation:

Configure the macOS system to disable Remote Management with the following commands:

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources
/kickstart -deactivate -stop
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.115 APPL-15-002260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the Bluetooth System Settings pane.

```
GROUP ID: V-268532
RULE ID: SV-268532r1034536
```

Rationale:

The Bluetooth System Setting pane must be disabled to prevent access to the Bluetooth configuration.

Audit:

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.

Remediation:

Configure the macOS system to disable the Bluetooth System Settings pane by installing the "com.apple.systempreferences" configuration profiles.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.116 APPL-15-002270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the iCloud Freeform services.

```
GROUP ID: V-268533
RULE ID: SV-268533r1034539
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable iCloud Freeform services by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.117 APPL-15-002271 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable iPhone Mirroring.

```
GROUP ID: V-272477
RULE ID: SV-272477r1069484
```

Rationale:

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

Audit:

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.

Remediation:

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

Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

Internal Only - General

1.118 APPL-15-003001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must issue or obtain public key certificates from an approved service provider.

```
GROUP ID: V-268534
RULE ID: SV-268534r1034542
```

Rationale:

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

Audit:

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.

Remediation:

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.

Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

CCI-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5::SC-17 b

Internal Only - General

1.119 APPL-15-003007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must require that passwords contain a minimum of one numeric character.

```
GROUP ID: V-268535
RULE ID: SV-268535r1034545
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

Internal Only - General

1.120 APPL-15-003008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must restrict maximum password lifetime to 60 days.

```
GROUP ID: V-268536
RULE ID: SV-268536r1038967
```

Rationale:

The macOS must be configured to enforce a maximum password lifetime limit of at least 60 days.

This rule ensures that users are forced to change their passwords frequently enough to prevent malicious users from gaining and maintaining access to the system.

NOTE: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B 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.

Audit:

Verify the macOS system is configured to restrict maximum password lifetime to 60 days with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |
/usr/bin/xmllint --xpath
'//dict/key[text()="policyAttributeExpiresEveryNDays"]/following-
sibling::*[1]/text()' -
```

If the result is not "60" or less, this is a finding.

Remediation:

Configure the macOS system to restrict maximum password lifetime to 60 days by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

Internal Only - General

1.121 APPL-15-003010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must require a minimum password length of 14 characters.

```
GROUP ID: V-268537
RULE ID: SV-268537r1034551
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to enforce a 14-character password length by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

Internal Only - General

1.122 APPL-15-003011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must require that passwords contain a minimum of one special character.

```
GROUP ID: V-268538
RULE ID: SV-268538r1034554
```

Rationale:

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 should be organizationally defined. The values defined are based on common complexity values, but each organization may define its own password complexity rules.

Audit:

Verify the macOS system is configured to require passwords contain a minimum of one special character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 |
/usr/bin/xmllint --xpath
'boolean(//*[contains(text(),"policyAttributePassword matches '\''(.*[^a-zA-
Z0-9].*){1,}'\''")])' -
```

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

Remediation:

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

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

Internal Only - General

1.123 APPL-15-003012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable password hints.

```
GROUP ID: V-268539
RULE ID: SV-268539r1034557
```

Rationale:

Password hints must be disabled.

Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

Audit:

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.

Remediation:

Configure the macOS system to disable password hints by installing the "com.apple.loginwindow" configuration profile.

Additional Information:

CCI-000206 Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

- NIST SP 800-53::IA-6
- NIST SP 800-53A::IA-6.1
- NIST SP 800-53 Revision 4::IA-6
- NIST SP 800-53 Revision 5::IA-6

Internal Only - General

1.124 APPL-15-003013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enable firmware password.

```
GROUP ID: V-268540
RULE ID: SV-268540r1034560
```

Rationale:

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.

Audit:

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.

Internal Only - General

Remediation:

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.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.125 APPL-15-003014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must remove password hints from user accounts.

```
GROUP ID: V-268541
RULE ID: SV-268541r1034563
```

Rationale:

User accounts must not contain password hints.

Password hints leak information about passwords in use and can lead to loss of confidentiality.

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000206 Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

- NIST SP 800-53::IA-6
- NIST SP 800-53A::IA-6.1
- NIST SP 800-53 Revision 4::IA-6
- NIST SP 800-53 Revision 5::IA-6

Internal Only - General

1.126 APPL-15-003020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce smart card authentication.

```
GROUP ID: V-268542
RULE ID: SV-268542r1034566
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

Internal Only - General

1.127 APPL-15-003030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must allow smart card authentication.

```
GROUP ID: V-268543
RULE ID: SV-268543r1034569
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (c)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (2)

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

Internal Only - General

1.128 APPL-15-003050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce multifactor authentication for login.

```
GROUP ID: V-268544
RULE ID: SV-268544r1034572
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

Internal Only - General

1.129 APPL-15-003051 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce multifactor authentication for the su command.

```
GROUP ID: V-268545
RULE ID: SV-268545r1034575
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

Internal Only - General

1.130 APPL-15-003052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce multifactor authentication for privilege escalation through the sudo command.

```
GROUP ID: V-268546
RULE ID: SV-268546r1034578
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

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
```

Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

Internal Only - General

1.131 APPL-15-003060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must require that passwords contain a minimum of one lowercase character and one uppercase character.

```
GROUP ID: V-268547
RULE ID: SV-268547r1034581
```

Rationale:

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

Audit:

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.

Remediation:

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.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-004065 For password-based authentication, employ automated tools to assist the user in selecting strong password authenticators.

- NIST SP 800-53 Revision 5::IA-5 (1) (g)

Internal Only - General

1.132 APPL-15-003070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must set minimum password lifetime to 24 hours.

```
GROUP ID: V-268548
RULE ID: SV-268548r1034796
```

Rationale:

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 should be organizationally defined. The values defined are based on common complexity values, but each organization may define its own password complexity rules.

Audit:

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.

Internal Only - General

Remediation:

Configure the macOS system to set minimum password lifetime to 24 hours.
This setting may be enforced using local policy or by a directory service.
To set local policy to require a minimum password lifetime, edit the current password policy to contain the following 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
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

Internal Only - General

1.133 APPL-15-003080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable accounts after 35 days of inactivity.

```
GROUP ID: V-268549
RULE ID: SV-268549r1034798
```

Rationale:

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

Audit:

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.

Internal Only - General

Remediation:

Configure the macOS system to disable accounts after 35 days of inactivity with the following command:
This setting may be enforced using local policy or by a directory service.
To set local policy to disable an inactive user after 35 days, edit the current password policy to contain the following within the "policyCategoryAuthentication":
[source,xml]

```
<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
```

Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5::AC-2 (3) (b)

Internal Only - General

1.134 APPL-15-004001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure Apple System Log (ASL) files owned by root and group to wheel.

```
GROUP ID: V-268550
RULE ID: SV-268550r1034590
```

Rationale:

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

Audit:

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.

Remediation:

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}')
```


Internal Only - General

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.135 APPL-15-004002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure Apple System Log (ASL) files to mode 640 or less permissive.

```
GROUP ID: V-268551
RULE ID: SV-268551r1034593
```

Rationale:

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

Audit:

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.

Remediation:

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}')
```


Internal Only - General

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.136 APPL-15-004022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must require users to reauthenticate for privilege escalation when using the "sudo" command.

```
GROUP ID: V-274881
RULE ID: SV-274881r1099904
```

Rationale:

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

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

Internal Only - General

1.137 APPL-15-004030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure system log files owned by root and group to wheel.

```
GROUP ID: V-268552
RULE ID: SV-268552r1034596
```

Rationale:

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

Audit:

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.

Remediation:

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}')
```


Internal Only - General

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.138 APPL-15-004040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure system log files to mode 640 or less permissive.

```
GROUP ID: V-268553
RULE ID: SV-268553r1034599
```

Rationale:

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

Audit:

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.

Remediation:

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}')
```


Internal Only - General

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.139 APPL-15-004050 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The macOS system must configure install.log retention to 365.

```
GROUP ID: V-268554
RULE ID: SV-268554r1034602
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

Internal Only - General

1.140 APPL-15-004060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure sudoers timestamp type.

```
GROUP ID: V-274880
RULE ID: SV-274880r1099901
```

Rationale:

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

Audit:

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.

Remediation:

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' '{}' \;
```

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

Internal Only - General

1.141 APPL-15-005001 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must ensure System Integrity Protection is enabled.

```
GROUP ID: V-268555
RULE ID: SV-268555r1034605
```

Rationale:

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

Audit:

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.

Remediation:

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
```


Internal Only - General

Additional Information:

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

CCI-001496 Implement cryptographic mechanisms to protect the integrity of audit tools.

- NIST SP 800-53::AU-9 (3)
- NIST SP 800-53A::AU-9 (3).1
- NIST SP 800-53 Revision 4::AU-9 (3)
- NIST SP 800-53 Revision 5::AU-9 (3)

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

Internal Only - General

1.142 APPL-15-005020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The macOS system must enforce FileVault.

```
GROUP ID: V-268556
RULE ID: SV-268556r1034608
```

Rationale:

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

Audit:

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.

Remediation:

Refer to the FileVault supplemental to implement this rule.

Internal Only - General

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

Internal Only - General

1.143 APPL-15-005050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enable macOS Application Firewall.

```
GROUP ID: V-268557
RULE ID: SV-268557r1034611
```

Rationale:

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.

Audit:

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.

Remediation:

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

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.144 APPL-15-005052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must configure the login window to prompt for username and password.

```
GROUP ID: V-268558
RULE ID: SV-268558r1034614
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to prompt for username and password at the login window by installing the "com.apple.loginwindow" configuration profile.

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

Internal Only - General

1.145 APPL-15-005054 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the TouchID prompt during Setup Assistant.

```
GROUP ID: V-268559
RULE ID: SV-268559r1034617
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable the TouchID prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.146 APPL-15-005055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable the Screen Time prompt during Setup Assistant.

```
GROUP ID: V-268560
RULE ID: SV-268560r1034620
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable the Screen Time prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.147 APPL-15-005056 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Unlock with Apple Watch during Setup Assistant.

```
GROUP ID: V-268561
RULE ID: SV-268561r1034623
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Unlock with Apple Watch during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.148 APPL-15-005058 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Handoff.

```
GROUP ID: V-268562
RULE ID: SV-268562r1034626
```

Rationale:

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

Audit:

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.

Remediation:

Configure the macOS system to disable Handoff by installing the "com.apple.applicationaccess" configuration profile.

Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

Internal Only - General

1.149 APPL-15-005060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable proximity-based password sharing requests.

```
GROUP ID: V-268563
RULE ID: SV-268563r1034629
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable proximity-based password sharing requests by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.150 APPL-15-005061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Erase Content and Settings.

```
GROUP ID: V-268564
RULE ID: SV-268564r1034632
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to disable Erase Content and Settings by installing the "com.apple.applicationaccess" configuration profile.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.151 APPL-15-005070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enable Authenticated Root.

```
GROUP ID: V-268565
RULE ID: SV-268565r1034635
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.152 APPL-15-005080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must prohibit user installation of software into /users/.

```
GROUP ID: V-268566
RULE ID: SV-268566r1034638
```

Rationale:

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.yaml#L67-L70). Using these controls may not work as expected. Third party software may be required to fulfill the compliance requirements.

Audit:

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.applicationac
cess.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.

Internal Only - General

Remediation:

Configure the macOS system to prohibit user installation of software into /users/ by installing the "com.apple.applicationaccess.new" configuration profile.

Additional Information:

CCI-003980 Allow user installation of software only with explicit privileged status.

- NIST SP 800-53 Revision 5::CM-11 (2)

Internal Only - General

1.153 APPL-15-005090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must authorize USB devices before allowing connection.

```
GROUP ID: V-268567
RULE ID: SV-268567r1034641
```

Rationale:

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

Audit:

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.applicationac
cess')\
  .objectForKey('allowUSBRestrictedMode'))
    if ( pref1 == false ) {
      return("false")
    } else {
      return("true")
    }
  }
EOS
```

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

Remediation:

Configure the macOS system to authorize USB devices before allowing connection by installing the "com.apple.applicationaccess" configuration profile.

Internal Only - General

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5::CM-7 (9) (b)

Internal Only - General

1.154 APPL-15-005100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must ensure Secure Boot level is set to "full".

```
GROUP ID: V-268568
RULE ID: SV-268568r1034644
```

Rationale:

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

Audit:

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.

Remediation:

Configure the macOS system to ensure Secure Boot level is set to "full" by booting into Recovery Mode and enabling Full Secure Boot.

Internal Only - General

Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4::SI-6 a
- NIST SP 800-53 Revision 5::SI-6 a

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4::SI-6 b
- NIST SP 800-53 Revision 5::SI-6 b

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4::SI-6 d
- NIST SP 800-53 Revision 5::SI-6 d

Internal Only - General

1.155 APPL-15-005110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce enrollment in Mobile Device Management (MDM).

```
GROUP ID: V-268569
RULE ID: SV-268569r1034647
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system by ensuring that the system is enrolled via UAMDM.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.156 APPL-15-005120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enable Recovery Lock.

```
GROUP ID: V-268570
RULE ID: SV-268570r1034650
```

Rationale:

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.

Audit:

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.

Remediation:

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.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.157 APPL-15-005130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must enforce installation of XProtect Remediator and Gatekeeper updates automatically.

```
GROUP ID: V-268571
RULE ID: SV-268571r1034653
```

Rationale:

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.

Audit:

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.

Remediation:

Configure the macOS system to enforce installation of XProtect Remediator and Gatekeeper updates automatically by installing the "com.apple.SoftwareUpdate" configuration profile.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.158 APPL-15-005140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Genmoji.

```
GROUP ID: V-268572
RULE ID: SV-268572r1034656
```

Rationale:

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

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

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.159 APPL-15-005150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Apple Intelligence Image Generation.

```
GROUP ID: V-268573
RULE ID: SV-268573r1034659
```

Rationale:

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

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

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.160 APPL-15-005160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must disable Apple Intelligence Writing Tools.

```
GROUP ID: V-268574
RULE ID: SV-268574r1034662
```

Rationale:

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

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

Audit:

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.

Remediation:

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.161 APPL-15-999999 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The macOS system must be a supported release.

GROUP ID: V-268575
RULE ID: SV-268575r1034665

Rationale:

An operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Audit:

Verify the operating system version.
Click the Apple icon on the menu at the top left corner of the screen and select the "About This Mac" option.
The name of the macOS release installed appears on the Overview tab in the resulting window. The precise version number installed is displayed below that.
If the installed version of macOS 15 is not supported, this is a finding.

Remediation:

Upgrade to a supported version of the operating system.

Additional Information:

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

Internal Only - General

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	APPL-15-000001 (Manual)	☐	☐
1.2	APPL-15-000002 (Manual)	☐	☐
1.3	APPL-15-000003 (Manual)	☐	☐
1.4	APPL-15-000005 (Manual)	☐	☐
1.5	APPL-15-000007 (Manual)	☐	☐
1.6	APPL-15-000009 (Manual)	☐	☐
1.7	APPL-15-000012 (Manual)	☐	☐
1.8	APPL-15-000022 (Manual)	☐	☐
1.9	APPL-15-000014 (Manual)	☐	☐
1.10	APPL-15-000023 (Manual)	☐	☐
1.11	APPL-15-000024 (Manual)	☐	☐
1.12	APPL-15-000025 (Manual)	☐	☐
1.13	APPL-15-000030 (Manual)	☐	☐
1.14	APPL-15-000031 (Manual)	☐	☐
1.15	APPL-15-000033 (Manual)	☐	☐
1.16	APPL-15-000051 (Manual)	☐	☐
1.17	APPL-15-000052 (Manual)	☐	☐
1.18	APPL-15-000053 (Manual)	☐	☐
1.19	APPL-15-000054 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	APPL-15-000057 (Manual)	☐	☐
1.21	APPL-15-000060 (Manual)	☐	☐
1.22	APPL-15-000070 (Manual)	☐	☐
1.23	APPL-15-000090 (Manual)	☐	☐
1.24	APPL-15-000100 (Manual)	☐	☐
1.25	APPL-15-000110 (Manual)	☐	☐
1.26	APPL-15-000120 (Manual)	☐	☐
1.27	APPL-15-000130 (Manual)	☐	☐
1.28	APPL-15-000140 (Manual)	☐	☐
1.29	APPL-15-000160 (Manual)	☐	☐
1.30	APPL-15-000170 (Manual)	☐	☐
1.31	APPL-15-000180 (Manual)	☐	☐
1.32	APPL-15-000190 (Manual)	☐	☐
1.33	APPL-15-001001 (Manual)	☐	☐
1.34	APPL-15-001002 (Manual)	☐	☐
1.35	APPL-15-001003 (Manual)	☐	☐
1.36	APPL-15-001010 (Manual)	☐	☐
1.37	APPL-15-001012 (Manual)	☐	☐
1.38	APPL-15-001013 (Manual)	☐	☐
1.39	APPL-15-001014 (Manual)	☐	☐
1.40	APPL-15-001015 (Manual)	☐	☐
1.41	APPL-15-001016 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	APPL-15-001017 (Manual)	☐	☐
1.43	APPL-15-001020 (Manual)	☐	☐
1.44	APPL-15-001021 (Manual)	☐	☐
1.45	APPL-15-001022 (Manual)	☐	☐
1.46	APPL-15-001023 (Manual)	☐	☐
1.47	APPL-15-001024 (Manual)	☐	☐
1.48	APPL-15-001029 (Manual)	☐	☐
1.49	APPL-15-001030 (Manual)	☐	☐
1.50	APPL-15-001031 (Manual)	☐	☐
1.51	APPL-15-001044 (Manual)	☐	☐
1.52	APPL-15-001060 (Manual)	☐	☐
1.53	APPL-15-001100 (Manual)	☐	☐
1.54	APPL-15-001110 (Manual)	☐	☐
1.55	APPL-15-001120 (Manual)	☐	☐
1.56	APPL-15-001130 (Manual)	☐	☐
1.57	APPL-15-001140 (Manual)	☐	☐
1.58	APPL-15-001150 (Manual)	☐	☐
1.59	APPL-15-002001 (Manual)	☐	☐
1.60	APPL-15-002003 (Manual)	☐	☐
1.61	APPL-15-002004 (Manual)	☐	☐
1.62	APPL-15-002005 (Manual)	☐	☐
1.63	APPL-15-002006 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	APPL-15-002007 (Manual)	☐	☐
1.65	APPL-15-002008 (Manual)	☐	☐
1.66	APPL-15-002009 (Manual)	☐	☐
1.67	APPL-15-002010 (Manual)	☐	☐
1.68	APPL-15-002012 (Manual)	☐	☐
1.69	APPL-15-002013 (Manual)	☐	☐
1.70	APPL-15-002014 (Manual)	☐	☐
1.71	APPL-15-002015 (Manual)	☐	☐
1.72	APPL-15-002016 (Manual)	☐	☐
1.73	APPL-15-002017 (Manual)	☐	☐
1.74	APPL-15-002020 (Manual)	☐	☐
1.75	APPL-15-002021 (Manual)	☐	☐
1.76	APPL-15-002022 (Manual)	☐	☐
1.77	APPL-15-002023 (Manual)	☐	☐
1.78	APPL-15-002024 (Manual)	☐	☐
1.79	APPL-15-002035 (Manual)	☐	☐
1.80	APPL-15-002036 (Manual)	☐	☐
1.81	APPL-15-002037 (Manual)	☐	☐
1.82	APPL-15-002038 (Manual)	☐	☐
1.83	APPL-15-002039 (Manual)	☐	☐
1.84	APPL-15-002040 (Manual)	☐	☐
1.85	APPL-15-002041 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	APPL-15-002042 (Manual)	☐	☐
1.87	APPL-15-002043 (Manual)	☐	☐
1.88	APPL-15-002050 (Manual)	☐	☐
1.89	APPL-15-002052 (Manual)	☐	☐
1.90	APPL-15-002053 (Manual)	☐	☐
1.91	APPL-15-002060 (Manual)	☐	☐
1.92	APPL-15-002062 (Manual)	☐	☐
1.93	APPL-15-002063 (Manual)	☐	☐
1.94	APPL-15-002064 (Manual)	☐	☐
1.95	APPL-15-002066 (Manual)	☐	☐
1.96	APPL-15-002068 (Manual)	☐	☐
1.97	APPL-15-002069 (Manual)	☐	☐
1.98	APPL-15-002080 (Manual)	☐	☐
1.99	APPL-15-002090 (Manual)	☐	☐
1.100	APPL-15-002100 (Manual)	☐	☐
1.101	APPL-15-002110 (Manual)	☐	☐
1.102	APPL-15-002120 (Manual)	☐	☐
1.103	APPL-15-002130 (Manual)	☐	☐
1.104	APPL-15-002140 (Manual)	☐	☐
1.105	APPL-15-002150 (Manual)	☐	☐
1.106	APPL-15-002160 (Manual)	☐	☐
1.107	APPL-15-002170 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	APPL-15-002180 (Manual)	☐	☐
1.109	APPL-15-002200 (Manual)	☐	☐
1.110	APPL-15-002210 (Manual)	☐	☐
1.111	APPL-15-002220 (Manual)	☐	☐
1.112	APPL-15-002230 (Manual)	☐	☐
1.113	APPL-15-002240 (Manual)	☐	☐
1.114	APPL-15-002250 (Manual)	☐	☐
1.115	APPL-15-002260 (Manual)	☐	☐
1.116	APPL-15-002270 (Manual)	☐	☐
1.117	APPL-15-002271 (Manual)	☐	☐
1.118	APPL-15-003001 (Manual)	☐	☐
1.119	APPL-15-003007 (Manual)	☐	☐
1.120	APPL-15-003008 (Manual)	☐	☐
1.121	APPL-15-003010 (Manual)	☐	☐
1.122	APPL-15-003011 (Manual)	☐	☐
1.123	APPL-15-003012 (Manual)	☐	☐
1.124	APPL-15-003013 (Manual)	☐	☐
1.125	APPL-15-003014 (Manual)	☐	☐
1.126	APPL-15-003020 (Manual)	☐	☐
1.127	APPL-15-003030 (Manual)	☐	☐
1.128	APPL-15-003050 (Manual)	☐	☐
1.129	APPL-15-003051 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	APPL-15-003052 (Manual)	☐	☐
1.131	APPL-15-003060 (Manual)	☐	☐
1.132	APPL-15-003070 (Manual)	☐	☐
1.133	APPL-15-003080 (Manual)	☐	☐
1.134	APPL-15-004001 (Manual)	☐	☐
1.135	APPL-15-004002 (Manual)	☐	☐
1.136	APPL-15-004022 (Manual)	☐	☐
1.137	APPL-15-004030 (Manual)	☐	☐
1.138	APPL-15-004040 (Manual)	☐	☐
1.139	APPL-15-004050 (Manual)	☐	☐
1.140	APPL-15-004060 (Manual)	☐	☐
1.141	APPL-15-005001 (Manual)	☐	☐
1.142	APPL-15-005020 (Manual)	☐	☐
1.143	APPL-15-005050 (Manual)	☐	☐
1.144	APPL-15-005052 (Manual)	☐	☐
1.145	APPL-15-005054 (Manual)	☐	☐
1.146	APPL-15-005055 (Manual)	☐	☐
1.147	APPL-15-005056 (Manual)	☐	☐
1.148	APPL-15-005058 (Manual)	☐	☐
1.149	APPL-15-005060 (Manual)	☐	☐
1.150	APPL-15-005061 (Manual)	☐	☐
1.151	APPL-15-005070 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	APPL-15-005080 (Manual)	☐	☐
1.153	APPL-15-005090 (Manual)	☐	☐
1.154	APPL-15-005100 (Manual)	☐	☐
1.155	APPL-15-005110 (Manual)	☐	☐
1.156	APPL-15-005120 (Manual)	☐	☐
1.157	APPL-15-005130 (Manual)	☐	☐
1.158	APPL-15-005140 (Manual)	☐	☐
1.159	APPL-15-005150 (Manual)	☐	☐
1.160	APPL-15-005160 (Manual)	☐	☐
1.161	APPL-15-999999 (Manual)	☐	☐

Internal Only - General

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release

Internal Only - General