CIS Solaris 11 X86 STIG Benchmark

v1.0.0 - 08-29-2025

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.

Table of Contents

Overview

Target Technology Details

Solaris 11 X86 Secure Technical Implementation Guide (STIG)

Version: 3 Release: 2 Benchmark

Date: 30 Jan 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 Solaris 11 X86 and are looking to comply with the STIG guidance.

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.

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.

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.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Solaris 11 X86.

Recommendations

1 STIG RULES

Oracle Solaris 11

Solaris 11 X86 Secure Technical Implementation Guide (STIG)

Version: 3 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 SOL-11.1-010040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must produce records containing sufficient information to establish the identity of any user/subject associated with the event.

```
GROUP ID: V-216011
RULE ID: SV-216011r986460
```

Rationale:

Enabling the audit system will produce records with accurate time stamps, source, user, and activity information. Without this information malicious activity cannot be accurately tracked.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone to be secured.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

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

audit condition = auditing

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone to be secured.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

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

1.2 SOL-11.1-010060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must support an audit reduction capability.

```
GROUP ID: V-219988
RULE ID: SV-219988r958768
```

Rationale:

Using the audit system will utilize the audit reduction capability. Without an audit reduction capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

1.3 SOL-11.1-010070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system records must be able to be used by a report generation capability.

```
GROUP ID: V-219989
RULE ID: SV-219989r958774
```

Rationale:

Enabling the audit system will produce records for use in report generation. Without an audit reporting capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

1.4 SOL-11.1-010080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must provide the capability to automatically process audit records for events of interest based upon selectable, event criteria.

```
GROUP ID: V-216014
RULE ID: SV-216014r958430
```

Rationale:

Without an audit reporting capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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)

1.5 SOL-11.1-010100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit records must provide data for all auditable events defined at the organizational level for the organization-defined information system components.

```
GROUP ID: V-216015
RULE ID: SV-216015r958442
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Without accurate time stamps, source, user, and activity information, malicious activity cannot be accurately tracked.

Without an audit reduction and reporting capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

1.6 SOL-11.1-010120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must generate audit records for the selected list of auditable events as defined in DoD list of events.

```
GROUP ID: V-216016
RULE ID: SV-216016r958446
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Without accurate time stamps, source, user, and activity information, malicious activity cannot be accurately tracked.

Without an audit reduction and reporting capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

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

1.7 SOL-11.1-010130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must support the capability to compile audit records from multiple components within the system into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance.

```
GROUP ID: V-219990
RULE ID: SV-219990r958442
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Without accurate time stamps, source, user, and activity information, malicious activity cannot be accurately tracked.

Without an audit reduction and reporting capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

1.8 SOL-11.1-010140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Audit records must include what type of events occurred.

```
GROUP ID: V-216018
RULE ID: SV-216018r958412
```

Rationale:

Without proper system auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

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

1.9 SOL-11.1-010150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Audit records must include when (date and time) the events occurred.

```
GROUP ID: V-216019
RULE ID: SV-216019r958414
```

Rationale:

Without accurate time stamps malicious activity cannot be accurately tracked.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

1.10 SOL-11.1-010160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Audit records must include where the events occurred.

```
GROUP ID: V-216020
RULE ID: SV-216020r958416
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Without accurate time stamps, source, user, and activity information, malicious activity cannot be accurately tracked.

Without an audit reduction and reporting capability, users find it difficult to identify specific patterns of attack.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

1.11 SOL-11.1-010170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Audit records must include the sources of the events that occurred.

```
GROUP ID: V-216021
RULE ID: SV-216021r958418
```

Rationale:

Without accurate source information malicious activity cannot be accurately tracked.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

1.12 SOL-11.1-010180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Audit records must include the outcome (success or failure) of the events that occurred.

```
GROUP ID: V-216022
RULE ID: SV-216022r958420
```

Rationale:

Tracking both the successful and unsuccessful attempts aids in identifying threats to the system.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getcond

If this command does not report:

audit condition = auditing

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

If auditing has been disabled, it must be enabled with the following command:

pfexec audit -s

Additional Information:

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

1.13 SOL-11.1-010220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must be configured to audit file deletions.

```
GROUP ID: V-216023
RULE ID: SV-216023r959010
```

Rationale:

Without auditing, malicious activity cannot be detected.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the OS version you are currently securing.

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active |cut -f2 -d=

If "fd" audit flag is not included in output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "fd" audit flag is not included in output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

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

1.14 SOL-11.1-010230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must be configured to audit account creation.

```
GROUP ID: V-216024
RULE ID: SV-216024r958368
```

Rationale:

Without auditing, malicious activity cannot be detected.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "ps" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

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)

1.15 SOL-11.1-010250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must be configured to audit account modification.

```
GROUP ID: V-216025
RULE ID: SV-216025r958590
```

Rationale:

Without auditing, malicious activity cannot be detected.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "ps" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

Additional Information:

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)

1.16 SOL-11.1-010260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must automatically audit account disabling actions.

```
GROUP ID: V-216026
RULE ID: SV-216026r958592
```

Rationale:

Without auditing, malicious activity cannot be detected.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "ps" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

Additional Information:

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)

1.17 SOL-11.1-010270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must automatically audit account termination.

```
GROUP ID: V-216027
RULE ID: SV-216027r958594
```

Rationale:

Without auditing, malicious activity cannot be detected.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "ps" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

Additional Information:

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)

1.18 SOL-11.1-010290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must ensure unauthorized, security-relevant configuration changes detected are tracked.

```
GROUP ID: V-216028
RULE ID: SV-216028r959010
```

Rationale:

Without auditing, malicious activity cannot be detected.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "as" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

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

1.19 SOL-11.1-010300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must be configured to audit all administrative, privileged, and security actions.

```
GROUP ID: V-216029
RULE ID: SV-216029r959010
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "as" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

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

1.20 SOL-11.1-010310 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The audit system must be configured to audit login, logout, and session initiation.

```
GROUP ID: V-216030
RULE ID: SV-216030r958406
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

The Audit Configuration profile is required.

Check that the audit flag for auditing login and logout is enabled.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the OS version you are currently securing.

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "lo" audit flag is not included in output, this is a finding

pfexec auditconfig -getnaflags | grep active | cut -f2 -d=

If "na" and "lo" audit flags are not included in output, this is a finding

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa" or if the "ft,lo,ap,ss,as,ua,pe” audit flag(s) are not included in output, this is a finding

pfexec auditconfig -t -getnaflags | cut -f2 -d=

If "na" and "lo" audit flags are not included in output, this is a finding

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

pfexec auditconfig -setnaflags lo,na

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

pfexec auditconfig -setnaflags lo,na

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

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)

1.21 SOL-11.1-010320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must be configured to audit all discretionary access control permission modifications.

```
GROUP ID: V-219991
RULE ID: SV-219991r958442
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

The Audit Configuration profile is required.

Check that the audit flag for auditing file access is enabled.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the OS version you are currently securing.

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "fm" audit flag is not included in output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "fm" audit flag is not included in output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

Additional Information:

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

1.22 SOL-11.1-010330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must be configured to audit the loading and unloading of dynamic kernel modules.

```
GROUP ID: V-219992
RULE ID: SV-219992r958442
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global", this check applies.

Determine the OS version currently being secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "as" audit flag is not included in the output, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "cusa,fm,fd,-fa,-ps,-ex" audit flags are not included in the output, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone currently being secured.

zonename

If the command output is "global ", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

Additional Information:

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

1.23 SOL-11.1-010340 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The audit system must be configured to audit failed attempts to access files and programs.

```
GROUP ID: V-216033
RULE ID: SV-216033r959010
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

The Audit Configuration profile is required.

Check that the audit flag for auditing file access is enabled.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the OS version you are currently securing.

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -getflags | grep active | cut -f2 -d=

If "-fa" and "-ps" audit flags are not displayed, this is a finding.

For Solaris 11.4 or newer:

pfexec auditconfig -t -getflags | cut -f2 -d=

If "-fa", "-ex", and "-ps" audit flags are not displayed, this is a finding.

Determine if auditing policy is set to collect command line arguments.

pfexec auditconfig -getpolicy | grep active | grep argv

If the active audit policies line does not appear, this is a finding.

Remediation:

The Audit Configuration profile is required. All audit flags must be enabled in a single command.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec auditconfig -setflags cusa,-ps,fd,-fa,fm

For Solaris 11.4 or newer:

pfexec auditconfig -setflags cusa,-fa,-ex,-ps,fd,fm

Enable the audit policy to collect command line arguments.

pfexec auditconfig -setpolicy +argv

These changes will not affect users that are currently logged in.

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

1.24 SOL-11.1-010350 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must protect against an individual falsely denying having performed a particular action. In order to do so the system must be configured to send audit records to a remote audit server.

```
GROUP ID: V-216034
RULE ID: SV-216034r958440
```

Rationale:

Keeping audit records on a remote system reduces the likelihood of audit records being changed or corrupted. Duplicating and protecting the audit trail on a separate system reduces the likelihood of an individual being able to deny performing an action.

Solaris has supported rsyslog since version 11.1 and the differences between syslog and rsyslog are numerous. Solaris 11.4 installs rsyslog by default, but previous versions require a manual installation. When establishing a rsyslog server to forward to, it is important to consider the network requirements for this action. Note the following configuration options: There are three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above. Examples of each configuration: UDP *.* @remotesystemname TCP *.* @@remotesystemname RELP *.* :omrelp:remotesystemname:2514 Please note that a port number was given as there is no standard port for RELP.

Audit:

Audit Configuration rights profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check that the syslog audit plugin is enabled.

pfexec auditconfig -getplugin | grep audit_syslog

If "inactive" appears, this is a finding.

Determine which system-log service instance is online.

pfexec svcs system-log

Check that the /etc/syslog.conf or /etc/rsyslog.conf file is configured properly:

grep audit.notice /etc/syslog.conf

or

grep @@ /etc/rsyslog.conf

If

audit.notice @remotesystemname , audit.notice !remotesystemname (syslog configuration)

or

. @@remotesystemname (rsyslog configuration)

points to an invalid remote system or is commented out, this is a finding.

If no output is produced, this is a finding.

Check the remote syslog host to ensure that audit records can be found for this host.

Remediation:

Service Management, Audit Configuration and Audit Control rights profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Configure Solaris 11 to use the syslog audit plugin

pfexec auditconfig -setplugin audit_syslog active

Determine which system-log service instance is online.

pfexec svcs system-log

If the default system-log service is online:

pfedit /etc/syslog.conf

Add the line:

audit.notice @[remotesystemname]

or

audit.notice ![remotesystemname]

Replacing the remote system name with the correct hostname.

If the rsyslog service is online, modify the /etc/rsyslog.conf file.

pfedit /etc/rsyslog.conf

Add the line:

. @@[remotesystemname]

Or

. :omrelp:[remotesystemname]:[designatedportnumber]

Replacing the remote system name with the correct hostname.

Create the log file on the remote system

touch /var/adm/auditlog

Refresh the syslog service

pfexec svcadm refresh system/system-log:default

or

pfexec svcadm refresh system/system-log:rsyslog

Refresh the audit service

pfexec audit -s

Additional Information:

CCI-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

- NIST SP 800-53::AU-10
- NIST SP 800-53A::AU-10.1
- NIST SP 800-53 Revision 4::AU-10
- NIST SP 800-53 Revision 5::AU-10

1.25 SOL-11.1-010360 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The auditing system must not define a different auditing level for specific users.

```
GROUP ID: V-216035
RULE ID: SV-216035r959010
```

Rationale:

Without auditing, individual system accesses cannot be tracked, and malicious activity cannot be detected and traced back to an individual account.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

For each user on the system (not including root), check to see if special auditing flag configurations are set.

userattr audit_flags [username]

If any flags are returned, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

For each user on the system, remove all special audit configuration flags.

usermod -K audit_flags= [username]

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

1.26 SOL-11.1-010370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit system must alert the SA when the audit storage volume approaches its capacity.

```
GROUP ID: V-219993
RULE ID: SV-219993r971542
```

Rationale:

Filling the audit storage area can result in a denial of service or system outage and can lead to events going undetected.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The root role is required.

Verify the presence of an audit_warn entry in /etc/mail/aliases.

/usr/lib/sendmail -bv audit_warn

If the response is:

audit_warn... User unknown

this is a finding.

Review the output of the command and verify that the audit_warn alias notifies the appropriate users in this form:

audit_warn:user1,user2

If an appropriate user is not listed, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Add an audit_warn alias to /etc/mail/aliases that will forward to designated system administrator(s).

pfedit /etc/mail/aliases

Insert a line in the form:

audit_warn:user1,user2

Put the updated aliases file into service.

newaliases

Additional Information:

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)

1.27 SOL-11.1-010380 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The audit system must alert the System Administrator (SA) if there is any type of audit failure.

```
GROUP ID: V-219994
RULE ID: SV-219994r958758
```

Rationale:

Proper alerts to system administrators and Information Assurance (IA) officials of audit failures ensure a timely response to critical system issues.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The root role is required.

Verify the presence of an audit_warn entry in /etc/mail/aliases.

/usr/lib/sendmail -bv audit_warn

If the response is:

audit_warn... User unknown

this is a finding.

Review the output of the command and verify that the audit_warn alias notifies the appropriate users in this form:

audit_warn:user1,user2

If an appropriate user is not listed, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Add an audit_warn alias to /etc/mail/aliases that will forward to designated system administrator(s).

pfedit /etc/mail/aliases

Insert a line in the form:

audit_warn:user1,user2

Put the updated aliases file into service.

newaliases

Additional Information:

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)

1.28 SOL-11.1-010390 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must alert designated organizational officials in the event of an audit processing failure.

```
GROUP ID: V-216038
RULE ID: SV-216038r958424
```

Rationale:

Proper alerts to system administrators and IA officials of audit failures ensure a timely response to critical system issues.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The root role is required.

Verify the presence of an audit_warn entry in /etc/mail/aliases.

/usr/lib/sendmail -bv audit_warn

If the response is:

audit_warn... User unknown

this is a finding.

Review the output of the command and verify that the audit_warn alias notifies the appropriate users in this form:

audit_warn:user1,user2

If an appropriate user is not listed, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Add an audit_warn alias to /etc/mail/aliases that will forward to designated system administrator(s).

pfedit /etc/mail/aliases

Insert a line in the form:

audit_warn:user1,user2

Put the updated aliases file into service.

newaliases

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

1.29 SOL-11.1-010400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must allocate audit record storage capacity.

```
GROUP ID: V-219995
RULE ID: SV-219995r958752
```

Rationale:

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

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Review the current audit file space limitations

pfexec auditconfig -getplugin audit_binfile

Plugin: audit_binfile (active)

The output of the command will appear in this form.

Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=2

If p_minfree is not equal to "2" of greater, this is a finding.

p_dir defines the current audit file system.

Note: By default in Solaris 11.1, /var/audit is a link to /var/share/audit which is mounted on rpool/VARSHARE.

Check that zfs compression is enabled for the audit file system.

zfs get compression [poolname/filesystemname]

If compression is off, this is a finding.

Check that a ZFS quota is enforced for the audit filesystem.

zfs get quota [poolname/filesystemname]

If quota is set to "none", this is a finding.

Ensure that a reservation of space is enforced on /var/share so that other users do not use up audit space.

zfs get quota,reservation [poolname/filesystemname]

If reservation is set to "none", this is a finding.

Remediation:

The Audit Configuration, Audit Control and ZFS File System Management profiles are required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Determine the audit system directory name:

pfexec auditconfig -getplugin audit_binfile

Plugin: audit_binfile (active)

The output of the command will appear in this form:

Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=1;

p_dir defines the current audit file system.

Note: By default in Solaris 11.1, /var/audit is a link to /var/share/audit which is mounted on rpool/VARSHARE.

Set a minimum percentage of free space on the audit_binfile plugin to 2%.

pfexec auditconfig -setplugin audit_binfile p_minfree=2

Restart the audit system.

pfexec audit -s

Enable compression for the audit filesystem.

pfexec zfs set compression=on [poolname/filesystemname]

Set a ZFS quota on the default /var/share filesystem for audit records to ensure that the root pool is not filled up with audit logs.

pfexec zfs set quota=XXG [poolname/filesystemname]

This commands sets the quota to XX Gigabytes. This value should be based upon organizational requirements.

Set a ZFS reservation on the default /var/share filesystem for audit records to ensure that the audit file system is guaranteed a fixed amount of storage.

pfexec zfs set reservation=XXG [poolname/filesystemname]

This commands sets the quota to XX Gigabytes. This value should be based upon organizational requirements.

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

1.30 SOL-11.1-010410 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must configure auditing to reduce the likelihood of storage capacity being exceeded.

```
GROUP ID: V-219996
RULE ID: SV-219996r958752
```

Rationale:

Overflowing the audit storage area can result in a denial of service or system outage.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the status of the audit system. It must be auditing.

pfexec auditconfig -getplugin

If the output of this command does not contain:

p_fsize=4M

this is a finding.

Remediation:

The Audit Control profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Set the size of a binary audit file to a specific size. The size is specified in megabytes.

pfexec auditconfig -setplugin audit_binfile p_fsize=4M

Restart the audit system.

pfexec 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

1.31 SOL-11.1-010420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must shut down by default upon audit failure (unless availability is an overriding concern).

```
GROUP ID: V-216041
RULE ID: SV-216041r1038966
```

Rationale:

Continuing to operate a system without auditing working properly can result in undocumented access or system changes.

Audit:

The Audit Configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

pfexec auditconfig -getpolicy | grep ahlt

If the output does not include "ahlt" as an active audit policy, this is a finding.

pfexec auditconfig -getpolicy | grep active | grep cnt

If the output includes "cnt" as an active audit policy, this is a finding.

Remediation:

The Audit Configuration profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Set audit policy to halt and suspend on failure.

pfexec auditconfig -setpolicy +ahlt

pfexec auditconfig -setpolicy -cnt

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

1.32 SOL-11.1-010440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect audit information from unauthorized access.

```
GROUP ID: V-216042
RULE ID: SV-216042r958434
```

Rationale:

If audit data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve.

To ensure the veracity of audit data, the operating system must protect audit information from unauthorized access.

Satisfies: SRG-OS-000057, SRG-OS-000058, SRG-OS-000059

Audit:

The root role is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check that the directory storing the audit files is owned by root and has permissions 750 or less.

Note: By default in Solaris 11.1, /var/audit is a link to /var/share/audit which is mounted on rpool/VARSHARE.

Determine the location of the audit trail files

pfexec auditconfig -getplugin audit_binfile

The output will appear in this form:

Plugin: audit_binfile (active)

Attributes: p_dir=/var/audit;p_fsize=0;p_minfree=1

The p_dir attribute defines the location of the audit directory.

ls -ld /var/share/audit

Check the audit directory is owned by root, group is root, and permissions are 750 (rwx r-- ---) or less. If the permissions are excessive, this is a finding.

Remediation:

Note: By default in Solaris 11.1, /var/audit is a link to /var/share/audit which is mounted on rpool/VARSHARE.

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Determine the location of the audit trail files

pfexec auditconfig -getplugin audit_binfile|

The output will appear in this form:

Plugin: audit_binfile (active)

Attributes: p_dir=/var/audit;p_fsize=0;p_minfree=1

The p_dir attribute defines the location of the audit directory.

chown root [directory]

chgrp root [directory]

chmod 750 [directory]

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

1.33 SOL-11.1-020010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The System packages must be up to date with the most recent vendor updates and security fixes.

```
GROUP ID: V-216045
RULE ID: SV-216045r959010
```

Rationale:

Failure to install security updates can provide openings for attack.

Audit:

The Software Installation Profile is required.

An up-to-date Solaris repository must be accessible to the system. Enter the command:

pkg publisher

to determine the current repository publisher. If a repository is not accessible, it may need to be locally installed and configured.

Check for Solaris software package updates:

pfexec pkg update -n

If the command does not report "No updates available for this image," this is a finding.

Remediation:

The Software Installation Profile is required.

An up-to-date Solaris repository must be accessible to the system. Enter the command:

pkg publisher

to determine the current repository publisher. If a repository is not accessible, it may need to be locally installed and configured.

Update system packages to the current version.

pfexec pkg update

A reboot may be required for the updates to take effect.

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

1.34 SOL-11.1-020020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must verify that package updates are digitally signed.

```
GROUP ID: V-219997
RULE ID: SV-219997r1016296
```

Rationale:

Digitally signed packages ensure that the source of the package can be identified.

Audit:

Determine what the signature policy is for pkg publishers:

pkg property | grep signature-policy

Check that output produces:

signature-policy verify

If the output does not confirm that signature-policy verify is active, this is a finding.

Remediation:

The Software Installation Profile is required.

Configure the package system to ensure that digital signatures are verified.

pfexec pkg set-property signature-policy verify

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

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

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

1.35 SOL-11.1-020030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect audit tools from unauthorized access.

```
GROUP ID: V-216047
RULE ID: SV-216047r958610
```

Rationale:

Failure to maintain system configurations may result in privilege escalation.

Audit:

The Software Installation Profile is required.

Determine what the signature policy is for pkg publishers:

pkg property | grep signature-policy

Check that output produces:

signature-policy verify

If the output does not confirm that signature-policy verify is active, this is a finding.

Check that package permissions are configured and signed per vendor requirements.

pkg verify

If the command produces any output unrelated to STIG changes, this is a finding.

There is currently a Solaris 11 bug 16267888 which reports pkg verify errors for a variety of python packages. These can be ignored.

Remediation:

The Software Installation Profile is required.

Configure the package system to ensure that digital signatures are verified.

pfexec pkg set-property signature-policy verify

Check that package permissions are configured per vendor requirements.

pfexec pkg verify

If any errors are reported unrelated to STIG changes, use:

pfexec pkg fix

to bring configuration settings and permissions into factory compliance.

Additional Information:

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

1.36 SOL-11.1-020040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect audit tools from unauthorized modification.

```
GROUP ID: V-216048
RULE ID: SV-216048r958612
```

Rationale:

Failure to maintain system configurations may result in privilege escalation.

Audit:

The Software Installation Profile is required.

Determine what the signature policy is for pkg publishers:

pkg property | grep signature-policy

Check that output produces:

signature-policy verify

If the output does not confirm that signature-policy verify is active, this is a finding.

Check that package permissions are configured and signed per vendor requirements.

pkg verify

If the command produces any output unrelated to STIG changes, this is a finding.

There is currently a Solaris 11 bug 16267888 which reports pkg verify errors for a variety of python packages. These can be ignored.

Remediation:

The Software Installation Profile is required.

Configure the package system to ensure that digital signatures are verified.

pfexec pkg set-property signature-policy verify

Check that package permissions are configured per vendor requirements.

pfexec pkg verify

If any errors are reported unrelated to STIG changes, use:

pfexec pkg fix

to bring configuration settings and permissions into factory compliance.

Additional Information:

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

1.37 SOL-11.1-020050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect audit tools from unauthorized deletion.

```
GROUP ID: V-216049
RULE ID: SV-216049r958614
```

Rationale:

Failure to maintain system configurations may result in privilege escalation.

Audit:

The Software Installation Profile is required.

Determine what the signature policy is for pkg publishers:

pkg property | grep signature-policy

Check that output produces:

signature-policy verify

If the output does not confirm that signature-policy verify is active, this is a finding.

Check that package permissions are configured and signed per vendor requirements.

pkg verify

If the command produces any output unrelated to STIG changes, this is a finding.

There is currently a Solaris 11 bug 16267888 which reports pkg verify errors for a variety of python packages. These can be ignored.

Remediation:

The Software Installation Profile is required.

Configure the package system to ensure that digital signatures are verified.

pfexec pkg set-property signature-policy verify

Check that package permissions are configured per vendor requirements.

pfexec pkg verify

If any errors are reported unrelated to STIG changes, use:

pfexec pkg fix

to bring configuration settings and permissions into factory compliance.

Additional Information:

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

1.38 SOL-11.1-020080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

System packages must be configured with the vendor-provided files, permissions, and ownerships.

```
GROUP ID: V-216050
RULE ID: SV-216050r958634
```

Rationale:

Failure to maintain system configurations may result in privilege escalation.

Audit:

The Software Installation Profile is required.

Determine what the signature policy is for pkg publishers:

pkg property | grep signature-policy

Check that output produces:

signature-policy verify

If the output does not confirm that signature-policy verify is active, this is a finding.

Check that package permissions are configured and signed per vendor requirements.

pkg verify

If the command produces any output unrelated to STIG changes, this is a finding.

There is currently a Solaris 11 bug 16267888 which reports pkg verify errors for a variety of python packages. These can be ignored.

Remediation:

The Software Installation Profile is required.

Configure the package system to ensure that digital signatures are verified.

pfexec pkg set-property signature-policy verify

Check that package permissions are configured per vendor requirements.

pfexec pkg verify

If any errors are reported unrelated to STIG changes, use:

pfexec pkg fix

to bring configuration settings and permissions into factory compliance.

Additional Information:

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)

1.39 SOL-11.1-020090 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The finger daemon package must not be installed.

```
GROUP ID: V-216051
RULE ID: SV-216051r959010
```

Rationale:

Finger is an insecure protocol.

Audit:

Determine if the finger package is installed.

pkg list service/network/finger

If an installed package named service/network/finger is listed, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall service/network/finger

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

1.40 SOL-11.1-020100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The legacy remote network access utilities daemons must not be installed.

```
GROUP ID: V-216052
RULE ID: SV-216052r959010
```

Rationale:

Legacy remote access utilities allow remote control of a system without proper authentication.

Audit:

Determine if the legacy remote access package is installed.

pkg list service/network/legacy-remote-utilities

If an installed package named service/network/legacy-remote-utilities is listed, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall service/network/legacy-remote-utilities

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

1.41 SOL-11.1-020110 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NIS package must not be installed.

```
GROUP ID: V-216053
RULE ID: SV-216053r959010
```

Rationale:

NIS is an insecure protocol.

Audit:

Determine if the NIS package is installed.

pkg list service/network/nis

If an installed package named "service/network/nis" is listed, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall service/network/nis

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

1.42 SOL-11.1-020120 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The pidgin IM client package must not be installed.

```
GROUP ID: V-216054
RULE ID: SV-216054r959010
```

Rationale:

Instant messaging is an insecure protocol.

Audit:

Determine if the pidgin package is installed.

pkg list communication/im/pidgin

If an installed package named communication/im/pidgin is listed, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall communication/im/pidgin

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

1.43 SOL-11.1-020130 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The FTP daemon must not be installed unless required.

```
GROUP ID: V-216055
RULE ID: SV-216055r959010
```

Rationale:

FTP is an insecure protocol.

Audit:

Determine if the FTP package is installed.

pkg list service/network/ftp

If an installed package named "service/network/ftp" is listed and not required for operations, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall service/network/ftp

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

1.44 SOL-11.1-020140 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The TFTP service daemon must not be installed unless required.

```
GROUP ID: V-216056
RULE ID: SV-216056r959010
```

Rationale:

TFTP is an insecure protocol.

Audit:

Determine if the TFTP package is installed.

pkg list service/network/tftp

If an installed package named "/service/network/tftp" is listed and not required for operations, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall install/installadm

pfexec pkg uninstall service/network/tftp

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

1.45 SOL-11.1-020150 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The telnet service daemon must not be installed unless required.

```
GROUP ID: V-216057
RULE ID: SV-216057r959010
```

Rationale:

Telnet is an insecure protocol.

Audit:

Determine if the telnet daemon package in installed.

pkg list service/network/telnet

If an installed package named "service/network/telnet" is listed and vntsd is not in use for LDoms, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall service/network/telnet

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

1.46 SOL-11.1-020160 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The UUCP service daemon must not be installed unless required.

```
GROUP ID: V-216058
RULE ID: SV-216058r959010
```

Rationale:

UUCP is an insecure protocol.

Audit:

Determine if the UUCP package is installed.

pkg list /service/network/uucp

If an installed package named "/service/network/uucp" is listed, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall /service/network/uucp

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

1.47 SOL-11.1-020170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The rpcbind service must be configured for local only services unless organizationally defined.

```
GROUP ID: V-216059
RULE ID: SV-216059r959010
```

Rationale:

The portmap and rpcbind services increase the attack surface of the system and should only be used when needed. The portmap or rpcbind services are used by a variety of services using remote procedure calls (RPCs). The organization may define and document the limited use of services (for example NFS) that may use these services with approval from their Authorizing Official.

Audit:

Check the status of the rpcbind service local_only property.

svcprop -p config/local_only network/rpc/bind

If the state is not "true", this is a finding, unless it is required for system operations, then this is not a finding.

Remediation:

The Service Management profile is required.

If services such as portmap or rpcbind are required for system operations, the operator must document the services used and obtain approval from their Authorizing Official. They should also document the method(s) of blocking all other remote accesses through tools like a firewall or tcp_wrappers.

Otherwise, configure the rpc/bind service for local only access.

svccfg -s network/rpc/bind setprop config/local_only=true

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

1.48 SOL-11.1-020180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The VNC server package must not be installed unless required.

```
GROUP ID: V-216060
RULE ID: SV-216060r959010
```

Rationale:

The VNC service uses weak authentication capabilities and provides the user complete graphical system access.

Audit:

Determine if the VNC server package is installed.

pkg list x11/server/xvnc

If an installed package named "x11/server/xvnc is listed" is listed, this is a finding.

Remediation:

The Software Installation Profile is required.

pfexec pkg uninstall x11/server/xvnc

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

1.49 SOL-11.1-020190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ automated mechanisms, per organization-defined frequency, to detect the addition of unauthorized components/devices into the operating system.

```
GROUP ID: V-219998
RULE ID: SV-219998r958794
```

Rationale:

Addition of unauthorized code or packages may result in data corruption or theft.

Audit:

The Software Installation Profile is required.

Display the installation history of packages on the system to ensure that no undesirable packages have been installed:

pkg history -o finish,user,operation,command |grep install

If the install command is listed as "/usr/bin/packagemanager", execute the command:

pkg history -l

to determine which packages were installed during package manager sessions.

If undocumented or unapproved packages have been installed, this is a finding.

Remediation:

The Software Installation Profile is required.

Review and report any unauthorized package installation operations.

If necessary, remove unauthorized packages.

pfexec pkg uninstall [package name]

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

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

1.50 SOL-11.1-020220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must be configured to provide essential capabilities.

```
GROUP ID: V-216062
RULE ID: SV-216062r958478
```

Rationale:

Operating systems are capable of providing a wide variety of functions and services. Execution must be disabled based on organization-defined specifications.

Audit:

Identify the packages installed on the system.

pkg list

Any unauthorized software packages listed in the output are a finding.

Remediation:

The Software Installation profile is required.

Identify packages installed on the system:

pkg list

uninstall unauthorized packages:

pfexec pkg uninstall [package name]

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

1.51 SOL-11.1-020230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ automated mechanisms to prevent program execution in accordance with the organization-defined specifications.

```
GROUP ID: V-219999
RULE ID: SV-219999r958804
```

Rationale:

Operating systems are capable of providing a wide variety of functions and services. Execution must be disabled based on organization-defined specifications.

Audit:

Identify the packages installed on the system.

pkg list

Any unauthorized software packages listed in the output are a finding.

Remediation:

The Software Installation profile is required.

Identify packages installed on the system:

pkg list

uninstall unauthorized packages:

pfexec pkg uninstall [package name]

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

1.52 SOL-11.1-020300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All run control scripts must have mode 0755 or less permissive.

```
GROUP ID: V-216064
RULE ID: SV-216064r959010
```

Rationale:

If the startup files are writable by other users, these users could modify the startup files to insert malicious commands into the startup files.

Audit:

Check run control script modes.

ls -lL /etc/rc* /etc/init.d /lib/svc/method

If any run control script has a mode more permissive than 0755, this is a finding.

Remediation:

Ensure all system startup files have mode 0755 or less permissive. Examine the rc files, and all files in the rc1.d (rc2.d, and so on) directories, and in the /etc/init.d and /lib/svc/method directories to ensure they are not world writable. If they are world writable, use the chmod command to correct the vulnerability and to research why.

Procedure:

chmod go-w

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

1.53 SOL-11.1-020310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All run control scripts must have no extended ACLs.

```
GROUP ID: V-216065
RULE ID: SV-216065r959010
```

Rationale:

If the startup files are writable by other users, these users could modify the startup files to insert malicious commands into the startup files.

Audit:

Verify run control scripts have no extended ACLs.

ls -lL /etc/rc* /etc/init.d

If the permissions include a "+", the file has an extended ACL and this is a finding.

Remediation:

Remove the extended ACL from the file.

chmod A- [run control script with extended ACL]

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

1.54 SOL-11.1-020320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Run control scripts executable search paths must contain only authorized paths.

```
GROUP ID: V-216066
RULE ID: SV-216066r959010
```

Rationale:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory or other relative paths, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, two consecutive colons, or a single period, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.

Audit:

Verify run control scripts' executable search paths.

Procedure:

find /etc/rc* /etc/init.d /lib/svc/method -type f -print | xargs grep -i PATH

This variable is formatted as a colon-separated list of directories.

If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is a finding.

If an entry begins with a character other than a slash (/), or has not been documented with the ISSO, this is a finding.

Remediation:

Edit the run control script and remove the relative path entries from the executable search path variable that have not been documented with the ISSO.

Edit the run control script and remove any empty path entries from the file.

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

1.55 SOL-11.1-020330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Run control scripts library search paths must contain only authorized paths.

```
GROUP ID: V-216067
RULE ID: SV-216067r959010
```

Rationale:

The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, two consecutive colons, or a single period, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.

Audit:

Verify run control scripts' library search paths.

find /etc/rc* /etc/init.d -type f -print | xargs grep LD_LIBRARY_PATH

This variable is formatted as a colon-separated list of directories.

If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding.

If an entry begins with a character other than a slash (/), or has not been documented with the ISSO, this is a finding.

Remediation:

Edit the run control script and remove the relative path entries from the library search path variables that have not been documented with the ISSO.

Edit the run control script and remove any empty path entries from the file.

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

1.56 SOL-11.1-020340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Run control scripts lists of preloaded libraries must contain only authorized paths.

```
GROUP ID: V-216068
RULE ID: SV-216068r959010
```

Rationale:

The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries to the current working directory that have not been authorized, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with a slash (/) are absolute paths.

Audit:

Verify run control scripts' library preload list.

Procedure:

find /etc/rc* /etc/init.d -type f -print | xargs grep LD_PRELOAD

This variable is formatted as a colon-separated list of paths.

If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding.

If an entry begins with a character other than a slash (/), or has not been documented with the ISSO, this is a finding.

Remediation:

Edit the run control script and remove the relative path entries from the library preload variables that have not been documented with the ISSO.

Edit the run control script and remove any empty path entries from the file.

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

1.57 SOL-11.1-020350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Run control scripts must not execute world writable programs or scripts.

```
GROUP ID: V-216069
RULE ID: SV-216069r959010
```

Rationale:

World writable files could be modified accidentally or maliciously to compromise system integrity.

Audit:

Check the permissions on the files or scripts executed from system startup scripts to see if they are world writable.

Create a list of all potential run command level scripts.

ls -l /etc/init.d/* /etc/rc* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 -d " "

Create a list of world writable files.

find / -perm -002 -type f >> WorldWritableFileList

Determine if any of the world writeable files in "WorldWritableFileList" are called from the run command level scripts.

Note: Depending upon the number of scripts vs. world writable files, it may be easier to inspect the scripts manually.

more ls -l /etc/init.d/* /etc/rc* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 -d " "

If any system startup script executes any file or script that is world writable, this is a finding.

Remediation:

Remove the world writable permission from programs or scripts executed by run control scripts.

Procedure:

chmod o-w

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

1.58 SOL-11.1-020360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All system start-up files must be owned by root.

```
GROUP ID: V-216070
RULE ID: SV-216070r959010
```

Rationale:

System start-up files not owned by root could lead to system compromise by allowing malicious users or applications to modify them for unauthorized purposes. This could lead to system and network compromise.

Audit:

Check run control scripts' ownership.

ls -lL /etc/rc* /etc/init.d

If any run control script is not owned by root, this is a finding.

Remediation:

Change the ownership of the run control script(s) with incorrect ownership.

chown root

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

1.59 SOL-11.1-020370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All system start-up files must be group-owned by root, sys, or bin.

```
GROUP ID: V-216071
RULE ID: SV-216071r959010
```

Rationale:

If system start-up files do not have a group owner of root or a system group, the files may be modified by malicious users or intruders.

Audit:

Check run control scripts' group ownership.

Procedure:

ls -lL /etc/rc* /etc/init.d

If any run control script is not group-owned by root, sys, or bin, this is a finding.

Remediation:

Change the group ownership of the run control script(s) with incorrect group ownership.

Procedure:

chgrp root

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

1.60 SOL-11.1-020380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

System start-up files must only execute programs owned by a privileged UID or an application.

```
GROUP ID: V-216072
RULE ID: SV-216072r959010
```

Rationale:

System start-up files executing programs owned by other than root (or another privileged user) or an application indicates the system may have been compromised.

Audit:

Determine the programs executed by system start-up files. Determine the ownership of the executed programs.

cat /etc/rc* /etc/init.d/* | more

Check the ownership of every program executed by the system start-up files.

ls -l

If any executed program is not owned by root, sys, bin, or in rare cases, an application account, this is a finding.

Remediation:

Change the ownership of the file executed from system startup scripts to root, bin, or sys.

chown root

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

1.61 SOL-11.1-020500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Any X Windows host must write .Xauthority files.

```
GROUP ID: V-216073
RULE ID: SV-216073r959010
```

Rationale:

.Xauthority files ensure the user is authorized to access the specific X Windows host. If .Xauthority files are not used, it may be possible to obtain unauthorized access to the X Windows host.

Audit:

If X Display Manager (XDM) is not used on the system, this is not applicable.

Determine if XDM is running.

Procedure:

ps -ef | grep xdm

If X Display Manager (XDM) is not used on the system, this is not applicable.

Determine if XDM is running.

Procedure:

ps -ef | grep xdm

Check for .Xauthority files being utilized by looking for such files in the home directory of a user that uses X.

Procedure:

cd ~someuser

ls -la .Xauthority

If the .Xauthority file does not exist, ask the SA if the user is using X Windows. If the user is utilizing X Windows and the .Xauthority file does not exist, this is a finding.

Remediation:

Ensure the X Windows host is configured to write .Xauthority files into user home directories.

Edit the Xaccess file. Ensure the line that writes the .Xauthority file is uncommented.

Additional Information:

CCI-000297 Review and update the baseline configuration of the system when required due to organization-defined circumstances.

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

1.62 SOL-11.1-020510 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All .Xauthority files must have mode 0600 or less permissive.

```
GROUP ID: V-216074
RULE ID: SV-216074r959010
```

Rationale:

.Xauthority files ensure the user is authorized to access the specific X Windows host. Excessive permissions may permit unauthorized modification of these files, which could lead to Denial of Service to authorized access or allow unauthorized access to be obtained.

Audit:

If X Display Manager (XDM) is not used on the system, this is not applicable.

Determine if XDM is running.

Procedure:

ps -ef | grep xdm

Check the file permissions for the .Xauthority files in the home directories of users of X.
Procedure:

cd ~<X user>

ls -lL .Xauthority

If the file mode is more permissive than 0600, this is finding.

Remediation:

Change the mode of the .Xauthority files.

Procedure:

chmod 0600 .Xauthority

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

CCI-000225 Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned organizational tasks.

- NIST SP 800-53::AC-6
- NIST SP 800-53A::AC-6.1
- NIST SP 800-53 Revision 4::AC-6
- NIST SP 800-53 Revision 5::AC-6

1.63 SOL-11.1-020520 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The .Xauthority files must not have extended ACLs.

```
GROUP ID: V-216075
RULE ID: SV-216075r959010
```

Rationale:

.Xauthority files ensure the user is authorized to access the specific X Windows host. Extended ACLs may permit unauthorized modification of these files, which could lead to Denial of Service to authorized access or allow unauthorized access to be obtained.

Audit:

If X Display Manager (XDM) is not used on the system, this is not applicable.

Determine if XDM is running.

Procedure:

ps -ef | grep xdm

Check the file permissions for the .Xauthority files.

ls -lL .Xauthority

If the permissions include a "+", the file has an extended ACL and this is a finding.

Remediation:

Remove the extended ACL from the file.

chmod A- .Xauthority

Additional Information:

CCI-000225 Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned organizational tasks.

- NIST SP 800-53::AC-6
- NIST SP 800-53A::AC-6.1
- NIST SP 800-53 Revision 4::AC-6
- NIST SP 800-53 Revision 5::AC-6

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

1.64 SOL-11.1-020530 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

X displays must not be exported to the world.

```
GROUP ID: V-216076
RULE ID: SV-216076r959010
```

Rationale:

Open X displays allow an attacker to capture keystrokes and to execute commands remotely. Many users have their X Server set to xhost +, permitting access to the X Server by anyone, from anywhere.

Audit:

If X Windows is not used on the system, this is not applicable.

Check the output of the xhost command from an X terminal.

Procedure:

```
$ xhost
```

If the output reports access control is enabled (and possibly lists the hosts that can receive X Window logins), this is not a finding. If the xhost command returns a line indicating access control is disabled, this is a finding.

NOTE: It may be necessary to define the display if the command reports it cannot open the display.

Procedure:

```
$ DISPLAY=MachineName:0.0; export DISPLAY
```

MachineName may be replaced with an Internet Protocol Address. Repeat the check procedure after setting the display.

Remediation:

If using an xhost-type authentication the xhost - command can be used to remove current trusted hosts and then selectively allow only trusted hosts to connect with xhost + commands. A cryptographically secure authentication, such as provided by the xauth program, is always preferred. Refer to your X11 server's documentation for further security information.

Additional Information:

CCI-000225 Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned organizational tasks.

- NIST SP 800-53::AC-6
- NIST SP 800-53A::AC-6.1
- NIST SP 800-53 Revision 4::AC-6
- NIST SP 800-53 Revision 5::AC-6

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

1.65 SOL-11.1-020540 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

.Xauthority or X*.hosts (or equivalent) file(s) must be used to restrict access to the X server.

```
GROUP ID: V-216077
RULE ID: SV-216077r959010
```

Rationale:

If access to the X server is not restricted, a user's X session may be compromised.

Audit:

If X Display Manager (XDM) is not used on the system, this is not applicable.

Determine if XDM is running.

Procedure:

ps -ef | grep xdm

Determine if xauth is being used.

Procedure:

xauth

xauth> list

If the above command sequence does not show any host other than the localhost, then xauth is not being used.

Search the system for an X*.hosts files, where * is a display number that may be used to limit X window connections.

If no files are found, X*.hosts files are not being used.

If the X*.hosts files contain any unauthorized hosts, this is a finding.

If both xauth and X*.hosts files are not being used, this is a finding.

Remediation:

Create an X*.hosts file, where * is a display number that may be used to limit X window connections.

Add the list of authorized X clients to the file.

Additional Information:

CCI-000297 Review and update the baseline configuration of the system when required due to organization-defined circumstances.

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

1.66 SOL-11.1-020550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The .Xauthority utility must only permit access to authorized hosts.

```
GROUP ID: V-216078
RULE ID: SV-216078r959010
```

Rationale:

If unauthorized clients are permitted access to the X server, a user's X session may be compromised.

Audit:

If X Display Manager (XDM) is not used on the system, this is not applicable.

Determine if XDM is running.

Procedure:

ps -ef | grep xdm

Check the X Window system access is limited to authorized clients.

Procedure:

xauth

xauth> list

Ask the SA if the clients listed are authorized.

If any are not, this is a finding.

Remediation:

Remove unauthorized clients from the xauth configuration.

Procedure:

xauth remove

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

CCI-000225 Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned organizational tasks.

- NIST SP 800-53::AC-6
- NIST SP 800-53A::AC-6.1
- NIST SP 800-53 Revision 4::AC-6
- NIST SP 800-53 Revision 5::AC-6

1.67 SOL-11.1-020560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

X Window System connections that are not required must be disabled.

```
GROUP ID: V-216079
RULE ID: SV-216079r959010
```

Rationale:

If unauthorized clients are permitted access to the X server, a user's X session may be compromised.

Audit:

Determine if the X Window system is running.

Procedure:

ps -ef |grep X

Ask the SA if the X Window system is an operational requirement. If it is not, this is a finding.

Remediation:

Disable the X Windows server on the system.

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

1.68 SOL-11.1-030010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The graphical login service provides the capability of logging into the system using an X-Windows type interface from the console. If graphical login access for the console is required, the service must be in local-only mode.

```
GROUP ID: V-216080
RULE ID: SV-216080r959010
```

Rationale:

Externally accessible graphical desktop software may open the system to remote attacks.

Audit:

Determine if the X11 server system is providing remote services on the network.

svcprop -p options/tcp_listen svc:/application/x11/x11-server

If the output of the command is "true" and network access to graphical user login is not required, this is a finding.

Remediation:

The System Administrator profile is required:

Configure the X11 server for local system only graphics access.

pfexec svccfg -s svc:/application/x11/x11-server setprop options/tcp_listen=false

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

1.69 SOL-11.1-030030 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Generic Security Services (GSS) must be disabled.

```
GROUP ID: V-216081
RULE ID: SV-216081r959010
```

Rationale:

This service should be disabled if it is not required.

Audit:

Determine the status of the Generic Security Services.

svcs -Ho state svc:/network/rpc/gss

If the GSS service is reported as online, this is a finding.

Remediation:

The Service Management profile is required:

Disable the GSS service.

pfexec svcadm disable svc:/network/rpc/gss

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

1.70 SOL-11.1-030040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Systems services that are not required must be disabled.

```
GROUP ID: V-216082
RULE ID: SV-216082r959010
```

Rationale:

Services that are enabled but not required by the mission may provide excessive access or additional attack vectors to penetrate the system.

Audit:

Determine all of the systems services that are enabled on the system.

svcs -a | grep online

Document all enabled services and disable any that are not required.

Remediation:

The Service Management profile is required:

Disable any other service not required.

pfexec svcadm disable [service name]

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

1.71 SOL-11.1-030050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

TCP Wrappers must be enabled and configured per site policy to only allow access by approved hosts and services.

```
GROUP ID: V-216083
RULE ID: SV-216083r959010
```

Rationale:

TCP Wrappers are a host-based access control system that allows administrators to control who has access to various network services based on the IP address of the remote end of the connection. TCP Wrappers also provide logging information via syslog about both successful and unsuccessful connections.

Audit:

Check that TCP Wrappers are enabled and the host.deny and host.allow files exist.

inetadm -p | grep tcp_wrappers

If the output of this command is "tcp_wrappers=FALSE", this is a finding.

ls /etc/hosts.deny

/etc/hosts.deny

ls /etc/hosts.allow

/etc/hosts.allow

If these files do not exist or do not contain the names of allowed or denied hosts, this is a finding.

Remediation:

The root role is required.

To enable TCP Wrappers, run the following commands:

1. Create and customize your policy in /etc/hosts.allow:
2. echo "ALL: [net]/[mask], [net]/[mask], ..." > /etc/hosts.allow

where each [net>/[mask> combination (for example, the Class C address block "192.168.1.0/255.255.255.0") can represent one network block in use by your organization that requires access to this system.

2. Create a default deny policy in /etc/hosts.deny:

echo "ALL: ALL" >/etc/hosts.deny

3. Enable TCP Wrappers for all services started by inetd:

inetadm -M tcp_wrappers=TRUE
The versions of SunSSH (0.5.11) and sendmail that ship with Solaris 11 will automatically use TCP Wrappers to filter access if a hosts.allow or hosts.deny file exists.
The use of OpenSSH access is controlled by the sshd_config file starting with Solaris 11.3.
SunSSH is removed starting with Solaris 11.4.

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

1.72 SOL-11.1-030060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction.

```
GROUP ID: V-220000
RULE ID: SV-220000r958548
```

Rationale:

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, audio recording devices).

Auto execution vulnerabilities can result in malicious programs being automatically executed. Examples of information system functionality providing the capability for automatic execution of code are Auto Run and Auto Play. Auto Run and Auto Play are components of the Microsoft Windows operating system that dictate what actions the system takes when a drive is mounted. This requirement is designed to address vulnerabilities that arise when mobile devices such as USB memory sticks or other mobile storage devices are automatically mounted and applications are automatically invoked without user knowledge or acceptance.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine if the removable media volume manager is running.

svcs -Ho state svc:/system/filesystem/rmvolmgr:default

If the output reports that the service is "online", this is a finding.

Remediation:

The Service Management profile is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Disable the rmvolmgr service.

pfexec svcadm disable svc:/system/filesystem/rmvolmgr:default

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.73 SOL-11.1-040010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

User passwords must be changed at least every 60 days.

```
GROUP ID: V-216086
RULE ID: SV-216086r1038967
```

Rationale:

Limiting the lifespan of authenticators limits the period of time an unauthorized user has access to the system while using compromised credentials and reduces the period of time available for password-guessing attacks to run against a single password.

Solaris 11.4 introduced new password security features that allow for a more granular approach to password duration parameters. The introduction of MAXDAYS, MINDAYS, and WARNDAYS allow the /etc/default/passwd configuration file to enforce a password change every 60 days.

Audit:

The root role is required.

Determine if user passwords are properly configured to be changed every 60 days.

Determine the OS version to be secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

logins -ox |awk -F: '($1 != "root" && $8 != "LK" && $8 != "NL" && ($11 > “56" || $11 < “1")) { print }'

If output is returned and the listed account is accessed via direct logon, this is a finding.

Check that /etc/default/password is configured to enforce password expiration every eight weeks or less.

grep "^MAXWEEKS=" /etc/default/passwd

If the command does not report MAXWEEKS=8 or less, this is a finding.

For Solaris 11.4 or newer:

logins -ox |awk -F: '($1 != "root" && $8 != "LK" && $8 != "NL" && ($11 > "60"|| $11 < "1")) { print }'

If output is returned and the listed account is accessed via direct logon, this is a finding.

Check that /etc/default/password is configured to enforce password expiration every 60 days or less.

Note: It is an error to set both the WEEKS and the DAYS variant for a given MIN/MAX/WARN variable.

grep "^MAXDAYS=" /etc/default/passwd

If the command does not report MAXDAYS=60 or less, this is a finding.

grep "^MAXWEEKS=" /etc/default/passwd

If output is returned, this is a finding.

Remediation:

The User Security role is required.

For Solaris 11, 11.1, 11.2, and 11.3:

Change each username to enforce 56 day password changes.

pfexec passwd -x 56 [username]

pfedit /etc/default/passwd

Search for MAXWEEKS. Change the line to read:

MAXWEEKS=8

For Solaris 11.4 or newer:

Change each username to enforce 60 day password changes.

pfexec passwd -x 60 [username]

pfedit /etc/default/passwd

Note: It is an error to set both the WEEKS and the DAYS variant for a given MIN/MAX/WARN variable.

Search for MAXDAYS. Change the line to read:

MAXDAYS=60

Search for MAXWEEKS. Change the line to read:

#MAXWEEKS=

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-000199 The information system enforces maximum password lifetime restrictions.

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

1.74 SOL-11.1-040020 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must automatically terminate temporary accounts within 72 hours.

```
GROUP ID: V-216087
RULE ID: SV-216087r958364
```

Rationale:

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

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

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

When temporary and emergency accounts are created, there is a risk the temporary account may remain in place and active after the need for the account no longer exists.

To address this, in the event temporary accounts are required, accounts designated as temporary in nature must be automatically terminated after 72 hours. Such a process and capability greatly reduces the risk of accounts being misused, hijacked, or data compromised.

Audit:

The root role is required.

Determine if an expiration date is set for temporary accounts.

logins -aox |awk -F: '($14 == "0") {print}'

This command produces a list of accounts with no expiration date set. If any of these accounts are temporary accounts, this is a finding.

logins -aox |awk -F: '($14 != "0") {print}'

This command produces a list of accounts with an expiration date set as defined in the last field. If any accounts have a date that is not within 72 hours, this is a finding.

Remediation:

The User Security role is required.

Apply an expiration date to temporary users.

pfexec usermod -e "[date]" [username]

Enter the date in the form mm/dd/yyyy such that it is within 72 hours.

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)

1.75 SOL-11.1-040030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce minimum password lifetime restrictions.

```
GROUP ID: V-216088
RULE ID: SV-216088r1016284
```

Rationale:

Passwords need to be changed at specific policy-based intervals; however, if the information system or application allows the user to immediately and continually change their password, then the password could be repeatedly changed in a short period of time, defeating the organization's policy regarding password reuse.

Solaris 11.4 introduced new password security features that allow for a more granular approach to password duration parameters. The introduction of MAXDAYS, MINDAYS, and WARNDAYS allow the /etc/default/passwd configuration file to enforce a minimum password lifetime of a single day.

Audit:

The root role is required.

Check whether the minimum time period between password changes for each user account is one day or greater.

Determine the OS version to be secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

logins -ox |awk -F: '($1 != "root" && $8 != "LK" && $8 != "NL" && $10 < "1") { print }'

If output is returned and the listed account is accessed via direct logon, this is a finding.

Check that /etc/default/password is configured to minimum password change time of one week.

grep "^MINWEEKS=" /etc/default/passwd

If the command does not report MINWEEKS=1 or more, this is a finding.

For Solaris 11.4 or newer:

logins -ox |awk -F: '($1 != "root" && $8 != "LK" && $8 != "NL" && $10 < "1") { print }'

If output is returned and the listed account is accessed via direct logon, this is a finding.

Check that /etc/default/password is configured to minimum password change time of one day.

Note: It is an error to set both the WEEKS and the DAYS variant for a given MIN/MAX/WARN variable.

grep "^MINDAYS=" /etc/default/passwd

If the command does not report MINDAYS=1 or more, this is a finding.

grep "^MINWEEKS=" /etc/default/passwd

If output is returned, this is a finding.

Remediation:

The root role is required.

For Solaris 11, 11.1, 11.2, and 11.3:

pfedit /etc/default/passwd file.

Locate the line containing:

MINWEEKS

Change the line to read:

MINWEEKS=1

Set the per-user minimum password change times by using the following command on each user account.

passwd -n [number of days] [accountname]

For Solaris 11.4 or newer:

pfedit /etc/default/passwd file.

Note: It is an error to set both the WEEKS and the DAYS variant for a given MIN/MAX/WARN variable.

Search for MINDAYS. Change the line to read:

MINDAYS=1

Search for MINWEEKS. Change the line to read:

#MINWEEKS=

Set the per-user minimum password change times by using the following command on each user account.

passwd -n [number of days] [accountname]

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-000198 The information system enforces minimum password lifetime restrictions.

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

1.76 SOL-11.1-040040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

User passwords must be at least 15 characters in length.

```
GROUP ID: V-216089
RULE ID: SV-216089r1016285
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting guessing and brute-force attacks.

Password length is one factor of several that helps to determine strength and how long it takes to crack a password. The shorter the password is, the lower the number of possible combinations that need to be tested before the password is compromised.

Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

Check the system password length setting.

grep ^PASSLENGTH /etc/default/passwd

If PASSLENGTH is not set to 15 or more, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Locate the line containing:

PASSLENGTH

Change the line to read:

PASSLENGTH=15

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-000205 The information system enforces minimum password length.

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

1.77 SOL-11.1-040060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must require at least eight characters be changed between the old and new passwords during a password change.

```
GROUP ID: V-216091
RULE ID: SV-216091r1016286
```

Rationale:

To ensure password changes are effective in their goals, the system must ensure old and new passwords have significant differences. Without significant changes, new passwords may be easily guessed based on the value of a previously compromised password.

Audit:

Check /etc/default/passwd to verify the MINDIFF setting.

grep ^MINDIFF /etc/default/passwd

If the setting is not present, or is less than eight, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Search for MINDIFF. Change the line to read:

MINDIFF=8

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-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

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

1.78 SOL-11.1-040070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must require passwords to contain at least one uppercase alphabetic character.

```
GROUP ID: V-216092
RULE ID: SV-216092r1016287
```

Rationale:

Complex passwords can reduce the likelihood of success of automated password-guessing attacks.

Audit:

Check the MINUPPER setting.

grep ^MINUPPER /etc/default/passwd

If MINUPPER is not set to one or more, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Locate the line containing:

MINUPPER

Change the line to read:

MINUPPER=1

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-000192 The information system enforces password complexity by the minimum number of upper case characters used.

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

1.79 SOL-11.1-040080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must enforce password complexity requiring that at least one lowercase character is used.

```
GROUP ID: V-216093
RULE ID: SV-216093r1016288
```

Rationale:

Complex passwords can reduce the likelihood of success of automated password-guessing attacks.

Audit:

Check the MINLOWER setting.

grep ^MINLOWER /etc/default/passwd

If MINLOWER is not set to one or more, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Locate the line containing:

MINLOWER

Change the line to read:

MINLOWER=1

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-000193 The information system enforces password complexity by the minimum number of lower case characters used.

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

1.80 SOL-11.1-040090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must require passwords to contain at least one numeric character.

```
GROUP ID: V-216094
RULE ID: SV-216094r1016289
```

Rationale:

Complex passwords can reduce the likelihood of success of automated password-guessing attacks.

Audit:

Check the MINDIGIT setting.

grep ^MINDIGIT /etc/default/passwd

If the MINDIGIT setting is less than one, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Locate the line containing:

MINDIGIT

Change the line to read:

MINDIGIT=1

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-000194 The information system enforces password complexity by the minimum number of numeric characters used.

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

1.81 SOL-11.1-040100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must require passwords to contain at least one special character.

```
GROUP ID: V-216095
RULE ID: SV-216095r1016290
```

Rationale:

Complex passwords can reduce the likelihood of success of automated password-guessing attacks.

Audit:

Check the MINSPECIAL setting.

grep ^MINSPECIAL /etc/default/passwd

If the MINSPECIAL setting is less than one, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd a

Locate the line containing:

MINSPECIAL

Change the line to read:

MINSPECIAL=1

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-001619 The information system enforces password complexity by the minimum number of special characters used.

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

1.82 SOL-11.1-040110 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must require passwords to contain no more than three consecutive repeating characters.

```
GROUP ID: V-216096
RULE ID: SV-216096r959010
```

Rationale:

Complex passwords can reduce the likelihood of success of automated password-guessing attacks.

Audit:

Check the MAXREPEATS setting.

grep ^MAXREPEATS /etc/default/passwd

If the MAXREPEATS setting is greater than 3, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Locate the line containing:

MAXREPEATS

Change the line to read:

MAXREPEATS=3

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

1.83 SOL-11.1-040120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must not have accounts configured with blank or null passwords.

```
GROUP ID: V-216097
RULE ID: SV-216097r959010
```

Rationale:

Complex passwords can reduce the likelihood of success of automated password-guessing attacks.

Audit:

The root role is required.

Determine if accounts with blank or null passwords exist.

logins -po

If any account is listed, this is a finding.

Remediation:

The root role is required.

Remove, lock, or configure a password for any account with a blank password.

passwd [username]

or

Use the passwd -l command to lock accounts that are not permitted to execute commands.

or

Use the passwd -N command to set accounts to be non-login.

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

1.84 SOL-11.1-040130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors.

```
GROUP ID: V-216098
RULE ID: SV-216098r1016291
```

Rationale:

Cryptographic hashes provide quick password authentication while not actually storing the password.

Audit:

Determine which cryptographic algorithms are configured.

grep ^CRYPT /etc/security/policy.conf

If the command output does not include the lines below, this is a finding.

CRYPT_DEFAULT=6

CRYPT_ALGORITHMS_ALLOW=5,6

Remediation:

The root role is required.

Configure the system to disallow the use of UNIX encryption and enable SHA256 as the default encryption hash.

pfedit /etc/security/policy.conf

Check that the following lines exist and are not commented out:

CRYPT_DEFAULT=6

CRYPT_ALGORITHMS_ALLOW=5,6

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- 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)

1.85 SOL-11.1-040140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must disable accounts after three consecutive unsuccessful login attempts.

```
GROUP ID: V-216099
RULE ID: SV-216099r958388
```

Rationale:

Allowing continued access to accounts on the system exposes them to brute-force password-guessing attacks.

Audit:

Verify RETRIES is set in the login file.

grep ^RETRIES /etc/default/login

If the output is not RETRIES=3 or fewer, this is a finding.

Verify the account locks after invalid login attempts.

grep ^LOCK_AFTER_RETRIES /etc/security/policy.conf

If the output is not LOCK_AFTER_RETRIES=YES, this is a finding.

For each user in the system, use the command:

userattr lock_after_retries [username]

to determine if the user overrides the system value. If the output of this command is "no", this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/login

Change the line:

#RETRIES=5

to read

RETRIES=3

pfedit /etc/security/policy.conf

Change the line containing

#LOCK_AFTER_RETRIES

to read:

LOCK_AFTER_RETRIES=YES

If a user has lock_after_retries set to "no", update the user's attributes using the command:

usermod -K lock_after_retries=yes [username]

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

1.86 SOL-11.1-040160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The delay between login prompts following a failed login attempt must be at least 4 seconds.

```
GROUP ID: V-216100
RULE ID: SV-216100r959010
```

Rationale:

As an immediate return of an error message, coupled with the capability to try again, may facilitate automatic and rapid-fire brute-force password attacks by a malicious user.

Audit:

Check the SLEEPTIME parameter in the /etc/default/login file.

grep ^SLEEPTIME /etc/default/login

If the output is not SLEEPTIME=4 or more, this is a finding.

Remediation:

The root role is required.

pfedit the /etc/default/login

Locate the line containing:

SLEEPTIME

Change the line to read:

SLEEPTIME=4

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

1.87 SOL-11.1-040170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must require users to re-authenticate to unlock a graphical desktop environment.

```
GROUP ID: V-216101
RULE ID: SV-216101r958400
```

Rationale:

Allowing access to a graphical environment when the user is not attending the system can allow unauthorized users access to the system.

Audit:

If the system is not running XWindows, this check does not apply.

Determine if the screen saver timeout is configured properly.

grep "^*timeout:" /usr/share/X11/app-defaults/XScreenSaver

If the output is not:

*timeout: 0:15:00

or a shorter time interval, this is a finding.

grep "^*lockTimeout:" /usr/share/X11/app-defaults/XScreenSaver

If the output is not:

*lockTimeout: 0:00:05

or a shorter time interval, this is a finding.

grep "^*lock:" /usr/share/X11/app-defaults/XScreenSaver

If the output is not:

*lock: True

this is a finding.

For each existing user, check the configuring of their personal .xscreensaver file.

grep "^timeout:" $HOME/.xscreensaver

If the output is not:

timeout: 0:15:00

or a shorter time interval, this is a finding.

grep "^lockTimeout:" $HOME/.xscreensaver

If the output is not:

lockTimeout: 0:00:05

or a shorter time interval, this is a finding.

grep "^lock:" $HOME/.xscreensaver

If the output is not:

lock: True

this is a finding.

Remediation:

The root role is required.

Edit the global screensaver configuration file to ensure 15 minute screen lock.

pfedit /usr/share/X11/app-defaults/XScreenSaver

Find the timeout control lines and change them to read:

*timeout: 0:15:00

*lockTimeout: 0:00:05

*lock: True

For each user on the system, edit their local $HOME/.xscreensaver file and change the timeout values.

pfedit $HOME/.xscreensaver

Find the timeout control lines and change them to read:

timeout: 0:15:00

lockTimeout: 0:00:05

lock: True

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

1.88 SOL-11.1-040180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Graphical desktop environments provided by the system must automatically lock after 15 minutes of inactivity.

```
GROUP ID: V-216102
RULE ID: SV-216102r958402
```

Rationale:

Allowing access to a graphical environment when the user is not attending the system can allow unauthorized users access to the system.

Audit:

If the system is not running XWindows, this check does not apply.

Determine if the screen saver timeout is configured properly.

grep "^*timeout:" /usr/share/X11/app-defaults/XScreenSaver

If the output is not:

*timeout: 0:15:00

this is a finding.

grep "^*lockTimeout:" /usr/share/X11/app-defaults/XScreenSaver

If the output is not:

*lockTimeout: 0:00:05

this is a finding.

grep "^*lock:" /usr/share/X11/app-defaults/XScreenSaver

If the output is not:

*lock: True

this is a finding.

For each existing user, check the configuration of their personal .xscreensaver file.

grep "^lock:" $HOME/.xscreensaver

If the output is not:

*lock: True

this is a finding.

grep "^lockTimeout:" $HOME/.xscreensaver

If the output is not:

*lockTimeout: 0:00:05

this is a finding.

Remediation:

The root role is required.

Edit the global screensaver configuration file to ensure 15 minute screen lock.

pfedit /usr/share/X11/app-defaults/XScreenSaver

Find the timeout control lines and change them to read:

*timeout: 0:15:00

*lockTimeout:0:00:05

*lock: True

For each user on the system, edit their local $HOME/.xscreensaver file and change the timeout values.

pfedit $HOME/.xscreensaver

Find the timeout control lines and change them to read:

timeout: 0:15:00

lockTimeout:0:00:05

lock: True

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

1.89 SOL-11.1-040190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must prevent the use of dictionary words for passwords.

```
GROUP ID: V-216103
RULE ID: SV-216103r959010
```

Rationale:

The use of common words in passwords simplifies password-cracking attacks.

Audit:

Check /etc/default/passwd for dictionary check configuration.

grep ^DICTION /etc/default/passwd

If the DICTIONLIST or DICTIONDBDIR settings are not present and are not set to:

DICTIONLIST=/usr/share/lib/dict/words

DICTIONDBDIR=/var/passwd

this is a finding.

Determine if the target files exist.

ls -l /usr/share/lib/dict/words /var/passwd

If the files defined by DICTIONLIST or DICTIONBDIR are not present or are empty, this is a finding.

Remediation:

The root role is required.

pfedit /etc/default/passwd

Insert the lines:

DICTIONLIST=/usr/share/lib/dict/words

DICTIONDBDIR=/var/passwd

Generate the password dictionary by running the mkpwdict command.

mkpwdict -s /usr/share/lib/dict/words

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

1.90 SOL-11.1-040200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must restrict the ability of users to assume excessive privileges to members of a defined group and prevent unauthorized users from accessing administrative tools.

```
GROUP ID: V-220001
RULE ID: SV-220001r958726
```

Rationale:

Allowing any user to elevate their privileges can allow them excessive control of the system tools.

Audit:

Verify the root user is configured as a role, rather than a normal user.

userattr type root

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

Verify at least one local user has been assigned the root role.

grep '[:;]roles=root[^;]*' /etc/user_attr

If no lines are returned, or no users are permitted to assume the root role, this is a finding.

Remediation:

The root role is required.

Convert the root user into a role.

usermod -K type=role root

Add the root role to authorized users' logins.

usermod -R +root [username]

Remove the root role from users who should not be authorized to assume it.

usermod -R -root [username]

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)

1.91 SOL-11.1-040230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator.

```
GROUP ID: V-216105
RULE ID: SV-216105r1016292
```

Rationale:

Allowing any user to elevate their privileges can allow them excessive control of the system tools.

Audit:

Verify the root user is configured as a role, rather than a normal user.

userattr type root

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

Verify at least one local user has been assigned the root role.

grep '[:;]roles=root[^;]*' /etc/user_attr

If no lines are returned, or no users are permitted to assume the root role, this is a finding.

Remediation:

The root role is required.

Convert the root user into a role.

usermod -K type=role root

Add the root role to authorized users' logins.

usermod -R +root [username]

Remove the root role from users who should not be authorized to assume it.

usermod -R -root [username]

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-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

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

1.92 SOL-11.1-040250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The default umask for system and users must be 077.

```
GROUP ID: V-216106
RULE ID: SV-216106r959010
```

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions.

Audit:

The root role is required.

Determine if the default umask is configured properly.

grep -i "^UMASK=" /etc/default/login

If "UMASK=077" is not displayed, this is a finding.

Check local initialization files:

cut -d: -f1 /etc/passwd | xargs -n1 -iUSER sh -c "grep umask ~USER/.*"

If this command does not output a line indicating "umask 077" for each user, this is a finding.

Remediation:

The root role is required.

Edit local and global initialization files containing "umask" and change them to use 077.

pfedit /etc/default/login

Insert the line

UMASK=077

pfedit [user initialization file]

Insert the line

umask 077

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

1.93 SOL-11.1-040260 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The default umask for FTP users must be 077.

```
GROUP ID: V-216107
RULE ID: SV-216107r959010
```

Rationale:

Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions.

Audit:

The package service/network/ftp must be installed for this check.

pkg list service/network/ftp

If the output of this command is:

pkg list: no packages matching 'service/network/ftp' installed

no further action is required.

Determine if the FTP umask is set to 077.

egrep -i "^UMASK" /etc/proftpd.conf | awk '{ print $2 }'

If 077 is not displayed, this is a finding.

Remediation:

The root role is required.

pkg list service/network/ftp

If the output of this command is:

pkg list: no packages matching 'service/network/ftp' installed

no further action is required. Otherwise, edit the FTP configuration file.

pfedit /etc/proftpd.conf

Locate the line containing:

Umask

Change the line to read:

Umask 077

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

1.94 SOL-11.1-040270 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The value mesg n must be configured as the default setting for all users.

```
GROUP ID: V-216108
RULE ID: SV-216108r959010
```

Rationale:

The "mesg n" command blocks attempts to use the "write" or "talk" commands to contact users at their terminals, but has the side effect of slightly strengthening permissions on the user's TTY device.

Audit:

Determine if "mesg n" is the default for users.

grep "^mesg" /etc/.login

grep "^mesg" /etc/profile

If either of these commands produces a line:

mesg y

this is a finding.

For each existing user on the system, enter the command:

mesg

If the command output is:

is y

this is a finding.

Remediation:

The root role is required.

Edit the default profile configuration files.

pfedit /etc/profile

pfedit /etc/.login

In each file add a new line:

mesg n

For each user on the system, enter the command:

mesg n

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

1.95 SOL-11.1-040280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

User accounts must be locked after 35 days of inactivity.

```
GROUP ID: V-216109
RULE ID: SV-216109r1016293
```

Rationale:

Attackers that are able to exploit an inactive account can potentially obtain and maintain undetected access to an application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained. Operating systems need to track periods of user inactivity and disable accounts after 35 days of inactivity. Such a process greatly reduces the risk that accounts will be hijacked, leading to a data compromise.

This policy does not apply to either emergency accounts or infrequently used accounts. Infrequently used accounts are local logon accounts used by system administrators when network or normal logon/access is not available. Emergency accounts are administrator accounts created in response to crisis situations.

Satisfies: SRG-OS-000003, SRG-OS-000118

Audit:

Determine whether the 35-day inactivity lock is configured properly.

useradd -D | xargs -n 1 | grep inactive |

awk -F= '{ print $2 }'

If the command returns a result other than 35, this is a finding.

The root role is required for the "logins" command.

For each configured user name and role name on the system, determine whether a 35-day inactivity period is configured. Replace [username] with an actual user name or role name.

logins -axo -l [username] | awk -F: '{ print $13 }'

If these commands provide output other than 35, this is a finding.

Remediation:

The root role is required.

Perform the following to implement the recommended state:

useradd -D -f 35

To set this policy on a user account, use the command(s):

usermod -f 35 [username]

To set this policy on a role account, use the command(s):

rolemod -f 35 [name]

Additional Information:

CCI-000017 Disable accounts when the accounts have been inactive for the organization-defined time-period.

- NIST SP 800-53::AC-2 (3)
- NIST SP 800-53A::AC-2 (3).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (3)
- NIST SP 800-53 Revision 5::AC-2 (3) (d)

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)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

1.96 SOL-11.1-040310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Login services for serial ports must be disabled.

```
GROUP ID: V-216112
RULE ID: SV-216112r959010
```

Rationale:

Login services should not be enabled on any serial ports that are not strictly required to support the mission of the system. This action can be safely performed even when console access is provided using a serial port.

Audit:

Determine if terminal login services are disabled.

svcs -Ho state svc:/system/console-login:terma

svcs -Ho state svc:/system/console-login:termb

If the system/console-login services are not "disabled", this is a finding.

Remediation:

The Service Operator profile is required.

Disable serial terminal services.

pfexec svcadm disable svc:/system/console-login:terma

pfexec svcadm disable svc:/system/console-login:termb

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

1.97 SOL-11.1-040320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The nobody access for RPC encryption key storage service must be disabled.

```
GROUP ID: V-216113
RULE ID: SV-216113r959010
```

Rationale:

If login by the user "nobody" is allowed for secure RPC, there is an increased risk of system compromise. If keyserv holds a private key for the "nobody" user, it will be used by key_encryptsession to compute a magic phrase which can be easily recovered by a malicious user.

Audit:

Determine if the rpc-authdes package is installed:

pkg list solaris/legacy/security/rpc-authdes

If the output of this command is:

pkg list: no packages matching 'solaris/legacy/security/rpc-authdes' installed

no further action is required.

Determine if "nobody" access for keyserv is enabled.

grep "^ENABLE_NOBODY_KEYS=" /etc/default/keyserv

If the output of the command is not:

ENABLE_NOBODY_KEYS=NO

this is a finding.

Remediation:

Determine if the rpc-authdes package is installed:

pkg list solaris/legacy/security/rpc-authdes

If the output of this command is:

pkg list: no packages matching 'solaris/legacy/security/rpc-authdes' installed

no further action is required.

The root role is required.

Modify the /etc/default/keyserv file.

pfedit /etc/default/keyserv

Locate the line:

#ENABLE_NOBODY_KEYS=YES

Change it to:

ENABLE_NOBODY_KEYS=NO

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

1.98 SOL-11.1-040330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

X11 forwarding for SSH must be disabled.

```
GROUP ID: V-216114
RULE ID: SV-216114r959010
```

Rationale:

As enabling X11 Forwarding on the host can permit a malicious user to secretly open another X11 connection to another remote client during the session and perform unobtrusive activities such as keystroke monitoring, if the X11 services are not required for the system's intended function, they should be disabled or restricted as appropriate to the user's needs.

Audit:

Determine if X11 Forwarding is enabled.

grep "^X11Forwarding" /etc/ssh/sshd_config

If the output of this command is not:

X11Forwarding no

this is a finding.

Remediation:

The root role is required.

Modify the sshd_config file.

pfedit /etc/ssh/sshd_config

Locate the line containing:

X11Forwarding

Change it to:

X11Forwarding no

Restart the SSH service.

svcadm restart svc:/network/ssh

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

1.99 SOL-11.1-040331 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The sshd server must bind the X11 forwarding server to the loopback address.

```
GROUP ID: V-233301
RULE ID: SV-233301r959010
```

Rationale:

As enabling X11 Forwarding on the host can permit a malicious user to secretly open another X11 connection to another remote client during the session and perform unobtrusive activities such as keystroke monitoring, if the X11 services are not required for the system's intended function, they should be disabled or restricted as appropriate to the user's needs. By default, sshd binds the forwarding server to the loopback address and sets the hostname part of the DISPLAY environment variable to “localhost”. This prevents remote hosts from connecting to the proxy display.

Audit:

Determine if the X11 forwarding server is bound to the loopback address.

grep "^X11UseLocalhost" /etc/ssh/sshd_config

If the output of this command is not:

X11UseLocalhost yes

this is a finding.

Remediation:

The root role is required.

Modify the sshd_config file.

vi /etc/ssh/sshd_config

Locate the line containing:

X11UseLocalhost

Change it to:

X11UseLocalhost yes

Restart the SSH service.

svcadm restart svc:/network/ssh

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

1.100 SOL-11.1-040340 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Consecutive login attempts for SSH must be limited to 3.

```
GROUP ID: V-216115
RULE ID: SV-216115r959010
```

Rationale:

Setting the authentication login limit to a low value will disconnect the attacker and force a reconnect, which severely limits the speed of such brute-force attacks.

Audit:

Determine if consecutive login attempts are limited to 3.

grep "^MaxAuthTries" /etc/ssh/sshd_config | grep -v Log

If the output of this command is not:

MaxAuthTries 6

this is a finding.

Note: Solaris SSH MaxAuthTries of 6 maps to 3 actual failed attempts.

Remediation:

The root role is required.

Modify the sshd_config file.

pfedit /etc/ssh/sshd_config

Locate the line containing:

MaxAuthTries

Change it to:

MaxAuthTries 6

Restart the SSH service.

svcadm restart svc:/network/ssh

Note: Solaris SSH MaxAuthTries of 6 maps to 3 actual failed attempts.

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

1.101 SOL-11.1-040350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The rhost-based authentication for SSH must be disabled.

```
GROUP ID: V-216116
RULE ID: SV-216116r959010
```

Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

Audit:

Determine if rhost-based authentication is enabled.

grep "^IgnoreRhosts" /etc/ssh/sshd_config

If the output is produced and it is not:

IgnoreRhosts yes

this is a finding.

If the IgnoreRhosts line does not exist in the file, the default setting of "Yes" is automatically used and there is no finding.

Remediation:

The root role is required.

Modify the sshd_config file

pfedit /etc/ssh/sshd_config

Locate the line containing:

IgnoreRhosts

Change it to:

IgnoreRhosts yes

Restart the SSH service.

svcadm restart svc:/network/ssh

This action will only set the IgnoreRhosts line if it already exists in the file to ensure that it is set to the proper value. If the IgnoreRhosts line does not exist in the file, the default setting of "Yes" is automatically used, so no additional changes are needed.

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

1.102 SOL-11.1-040360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Direct root account login must not be permitted for SSH access.

```
GROUP ID: V-216117
RULE ID: SV-216117r959010
```

Rationale:

The system should not allow users to log in as the root user directly, as audited actions would be non-attributable to a specific user.

Audit:

Determine if root login is disabled for the SSH service.

grep "^PermitRootLogin" /etc/ssh/sshd_config

If the output of this command is not:

PermitRootLogin no

this is a finding.

Remediation:

The root role is required.

Modify the sshd_config file

pfedit /etc/ssh/sshd_config

Locate the line containing:

PermitRootLogin

Change it to:

PermitRootLogin no

Restart the SSH service.

svcadm restart svc:/network/ssh

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

1.103 SOL-11.1-040370 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Login must not be permitted with empty/null passwords for SSH.

```
GROUP ID: V-216118
RULE ID: SV-216118r959010
```

Rationale:

Permitting login without a password is inherently risky.

Audit:

Determine if empty/null passwords are allowed for the SSH service.

grep "^PermitEmptyPasswords" /etc/ssh/sshd_config

If the output of this command is not:

PermitEmptyPasswords no

this is a finding.

Remediation:

The root role is required.

Modify the sshd_config file

pfedit /etc/ssh/sshd_config

Locate the line containing:

PermitEmptyPasswords

Change it to:

PermitEmptyPasswords no

Restart the SSH service.

svcadm restart svc:/network/ssh

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

1.104 SOL-11.1-040380 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must terminate the network connection associated with a communications session at the end of the session or after 10 minutes of inactivity.

```
GROUP ID: V-216119
RULE ID: SV-216119r970703
```

Rationale:

This requirement applies to both internal and external networks.

Terminating network connections associated with communications sessions means de-allocating associated TCP/IP address/port pairs at the operating system level.

The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.

Audit:

Determine if SSH is configured to disconnect sessions after 10 minutes of inactivity.

grep ClientAlive /etc/ssh/sshd_config

If the output of this command is not:

ClientAliveInterval 600

ClientAliveCountMax 0

this is a finding.

Remediation:

The root role is required.

Configure the system to disconnect SSH sessions after 10 minutes of inactivity.

Modify the sshd_config file:

pfedit /etc/ssh/sshd_config

Modify or add the lines containing:

ClientAliveInterval

ClientAliveCountMax

Change them to:

ClientAliveInterval 600

ClientAliveCountMax 0

Restart the SSH service:

svcadm restart svc:/network/ssh

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

1.105 SOL-11.1-040390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Host-based authentication for login-based services must be disabled.

```
GROUP ID: V-216120
RULE ID: SV-216120r959010
```

Rationale:

The use of .rhosts authentication is an insecure protocol and can be replaced with public-key authentication using Secure Shell. As automatic authentication settings in the .rhosts files can provide a malicious user with sensitive system credentials, the use of .rhosts files should be disabled.

Audit:

Note: This is the location for Solaris 11.1. For earlier versions, the information is in /etc/pam.conf.

Determine if host-based authentication services are enabled.

grep 'pam_rhosts_auth.so.1' /etc/pam.conf /etc/pam.d/*| grep -vc '^#'

If the returned result is not 0 (zero), this is a finding.

Remediation:

Note: This is the location for Solaris 11.1. For earlier versions, the information is in /etc/pam.conf.

The root role is required.

ls -l /etc/pam.d

to identify the various configuration files used by PAM.

Search each file for the pam_rhosts_auth.so.1 entry.

grep pam_rhosts_auth.so.1 [filename]

Identify the file with the line pam_hosts_auth.so.1 in it.

pfedit [filename]

Insert a comment character (#) at the beginning of the line containing "pam_hosts_auth.so.1".

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

1.106 SOL-11.1-040400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The use of FTP must be restricted.

```
GROUP ID: V-216121
RULE ID: SV-216121r959010
```

Rationale:

FTP is an insecure protocol that transfers files and credentials in clear text, and can be replaced by using SFTP. However, if FTP is permitted for use in the environment, it is important to ensure that the default "system" accounts are not permitted to transfer files via FTP, especially the root role. Consider also adding the names of other privileged or shared accounts that may exist on the system such as user "oracle" and the account which the web server process runs under.

Audit:

The root role is required.

Determine if the FTP server package is installed:

pkg list service/network/ftp

If the output of this command is:

pkg list: no packages matching 'service/network/ftp' installed

no further action is required.

If the FTP server is installed, determine if FTP access is restricted.

for user in `logins -s | awk '{ print $1 }'`

aiuser noaccess nobody nobody4; do

grep -w "${user}" /etc/ftpd/ftpusers >/dev/null 2>&1

if [$? != 0]; then

echo "User '${user}' not in /etc/ftpd/ftpusers."

fi

done

If output is returned, this is a finding.

Remediation:

The root role is required.

Determine if the FTP server package is installed:

pkg list service/network/ftp

If the output of this command is:

pkg list: no packages matching 'service/network/ftp' installed

no further action is required.

for user in `logins -s | awk '{ print $1 }'`

aiuser noaccess nobody nobody4; do

$(echo $user >> /etc/ftpd/ftpusers)

done

sort -u /etc/ftpd/ftpusers > /etc/ftpd/ftpusers.temp

mv /etc/ftpd/ftpusers.temp /etc/ftpd/ftpusers

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

1.107 SOL-11.1-040410 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The system must not allow autologin capabilities from the GNOME desktop.

```
GROUP ID: V-216122
RULE ID: SV-216122r959010
```

Rationale:

As automatic logins are a known security risk for other than "kiosk" types of systems, GNOME automatic login should be disabled in pam.conf.

Audit:

Determine if autologin is enabled for the GNOME desktop.

egrep "auth|account" /etc/pam.d/gdm-autologin | grep -vc ^#

If the command returns other than "0", this is a finding.

Remediation:

The root role is required.

Modify the /etc/pam.d/gdm-autologin file.

pfedit /etc/pam.d/gdm-autologin

Locate the lines:

auth required pam_unix_cred.so.1

auth sufficient pam_allow.so.1

account sufficient pam_allow.so.1

Change the lines to read:

#auth required pam_unix_cred.so.1

#auth sufficient pam_allow.so.1

#account sufficient pam_allow.so.1

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

1.108 SOL-11.1-040420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unauthorized use of the at or cron capabilities must not be permitted.

```
GROUP ID: V-216123
RULE ID: SV-216123r959010
```

Rationale:

On many systems, only the system administrator needs the ability to schedule jobs.

Even though a given user is not listed in the "cron.allow" file, cron jobs can still be run as that user. The "cron.allow" file only controls administrative access to the "crontab" command for scheduling and modifying cron jobs. Much more effective access controls for the cron system can be obtained by using Role-Based Access Controls (RBAC).

Audit:

Check that "at" and "cron" users are configured correctly.

ls /etc/cron.d/cron.deny

If cron.deny exists, this is a finding.

ls /etc/cron.d/at.deny

If at.deny exists, this is a finding.

cat /etc/cron.d/cron.allow

cron.allow should have a single entry for "root", or the cron.allow file is removed if using RBAC.

If any accounts other than root that are listed and they are not properly documented with the IA staff, this is a finding.

wc -l /etc/cron.d/at.allow | awk '{ print $1 }'

If the output is non-zero, this is a finding, or the at.allow file is removed if using RBAC.

Remediation:

The root role is required.

Modify the cron configuration files.

mv /etc/cron.d/cron.deny /etc/cron.d/cron.deny.temp

mv /etc/cron.d/at.deny /etc/cron.d/at.deny.temp

Skip the remaining steps only if using the “solaris.jobs.user” RBAC role.

echo root > /etc/cron.d/cron.allow

cp /dev/null /etc/cron.d/at.allow

chown root:root /etc/cron.d/cron.allow /etc/cron.d/at.allow

chmod 400 /etc/cron.d/cron.allow /etc/cron.d/at.allow

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

1.109 SOL-11.1-040430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Logins to the root account must be restricted to the system console only.

```
GROUP ID: V-216124
RULE ID: SV-216124r959010
```

Rationale:

Use an authorized mechanism such as RBAC and the "su" command to provide administrative access to unprivileged accounts. These mechanisms provide an audit trail in the event of problems.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine if root login is restricted to the console.

grep "^CONSOLE=/dev/console" /etc/default/login

If the output of this command is not:

CONSOLE=/dev/console

this is a finding.

Remediation:

The root role is required.

Modify the /etc/default/login file

pfedit /etc/default/login

Locate the line containing:

CONSOLE

Change it to read:

CONSOLE=/dev/console

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

1.110 SOL-11.1-040450 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system, upon successful logon, must display to the user the date and time of the last logon (access).

```
GROUP ID: V-216125
RULE ID: SV-216125r987814
```

Rationale:

Users need to be aware of activity that occurs regarding their account. Providing users with information regarding the date and time of their last successful login allows the user to determine if any unauthorized activity has occurred and gives them an opportunity to notify administrators.

Audit:

Determine if last login will be printed for SSH users.

grep PrintLastLog /etc/ssh/sshd_config

If PrintLastLog is found, not preceded with a "#" sign, and is set to "no", this is a finding.

PrintLastLog should either not exist (defaulting to yes) or exist and be set to yes.

Remediation:

The root role is required for this action.

pfedit /etc/ssh/sshd_config

Locate the line containing:

PrintLastLog no

and place a comment sign ("")at the beginning of the line or delete the line

PrintLastLog no

Restart the ssh service

pfexec svcadm restart svc:/network/ssh

Additional Information:

CCI-000052 Notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

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

1.111 SOL-11.1-040460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must provide the capability for users to directly initiate session lock mechanisms.

```
GROUP ID: V-216126
RULE ID: SV-216126r1016294
```

Rationale:

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

Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users may secure their account should the need arise for them to temporarily vacate the immediate physical vicinity.

Audit:

Determine whether the lock screen function works correctly.

For Solaris 11, 11.1, 11.2, and 11.3:

In the GNOME 2 desktop System >> Lock Screen.

For Solaris 11.4 or newer:

In the GNOME 3 desktop Status Menu (top right corner) >> Lock Icon, check that the screen locks and displays the "password" prompt.

Check that "Disable Screensaver" is not selected in the GNOME Screensaver preferences.

If the screen does not lock or the "Disable Screensaver" option is selected, this is a finding.

Remediation:

User-initiated session lock is accessible from the GNOME graphical desktop menu GNOME 2: System >> Lock Screen.

GNOME 3: Status Menu (top right corner) >> Lock Icon.

However, the user has the option to disable screensaver lock.

For Solaris 11, 11.1, 11.2, and 11.3:

In the GNOME 2 desktop: System >> Preferences >> Screensaver.

For Solaris 11.4 or newer:

If using the default GNOME desktop: Activities >> Show Applications >> select "Screensaver" icon.

If using the GNOME Classic desktop: Applications >> Other >> Screensaver.

Ensure that "Mode" is set to "Blank Screen only".

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

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

1.112 SOL-11.1-040470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system session lock mechanism, when activated on a device with a display screen, must place a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

```
GROUP ID: V-216127
RULE ID: SV-216127r958404
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the system but does not log out because of the temporary nature of the absence.

The session lock will also include an obfuscation of the display screen to prevent other users from reading what was previously displayed.

Audit:

For Solaris 11, 11.1, 11.2, and 11.3:

In the GNOME 2 desktop System >> Preferences >> Screensaver.

For Solaris 11.4 or newer:

If using the default GNOME desktop: Activities >> Show Applications >> select "Screensaver" icon.

If using the GNOME Classic desktop: Applications >> Other >> Screensaver menu item the user can select other screens or disable screensaver.

Check that "Disable Screensaver" is not selected in the Gnome Screensaver preferences.

If "Disable Screensaver" is selected or "Blank Screen Only" is not selected, this is a finding.

Remediation:

For Solaris 11, 11.1, 11.2, and 11.3:

In the GNOME 2 desktop: System >> Preferences >> Screensaver.

For Solaris 11.4 or newer:

If using the default GNOME desktop: Activities >> Show Applications >> select “Screensaver” icon.

If using the GNOME Classic desktop: Applications >> Other >> Screensaver.

Click on Mode's pull-down.

Select: "Blank Screen Only".

Ensure that "Blank Screen Only" is selected.

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)

1.113 SOL-11.1-040480 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must not allow logins for users with blank passwords.

```
GROUP ID: V-216128
RULE ID: SV-216128r959010
```

Rationale:

If the password field is blank and the system does not enforce a policy that passwords are required, it could allow login without proper authentication of a user.

Audit:

Determine if the system is enforcing a policy that passwords are required.

grep ^PASSREQ /etc/default/login

If the command does not return:

PASSREQ=YES

this is a finding.

Remediation:

The root role is required.

Modify the /etc/default/login file.

pfedit /etc/default/login

Insert the line:

PASSREQ=YES

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

1.114 SOL-11.1-040490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent remote devices that have established a non-remote connection with the system from communicating outside of the communication path with resources in external networks.

```
GROUP ID: V-216129
RULE ID: SV-216129r959010
```

Rationale:

This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings not configurable by the user of the device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent split-tunneling. Split-tunneling might otherwise be used by remote users to communicate with the information system as an extension of the system and to communicate with local resources, such as a printer or file server. The remote device, when connected by a non-remote connection, becomes an extension of the information system allowing dual communications paths, such as split-tunneling, in effect allowing unauthorized external connections into the system. This is a split-tunneling requirement that can be controlled via the operating system by disabling interfaces.

Audit:

Determine if the "RestrictOutbound" profile is configured properly:

profiles -p RestrictOutbound info

If the output is not:

name=RestrictOutbound

desc=Restrict Outbound Connections

limitpriv=zone,!net_access

this is a finding.

For users who are not allowed external network access, determine if a user is configured with the "RestrictOutbound" profile.

profiles -l username

If the output does not include:

this is a finding.

Remediation:

The root Role is required.

Remove net_access privilege from users who may be accessing the systems externally.

1. Create an RBAC Profile with net_access restriction

profiles -p RestrictOutbound
profiles:RestrictOutbound> set desc="Restrict Outbound Connections"
profiles:RestrictOutbound> set limitpriv=zone,!net_access
profiles:RestrictOutbound> exit

2. Assign the RBAC Profile to a user

usermod -P +RestrictOutbound [username]
This prevents the user from initiating any outbound network connections.

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

1.115 SOL-11.1-040500 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must limit the number of concurrent sessions for each account to an organization-defined number of sessions.

```
GROUP ID: V-216130
RULE ID: SV-216130r958398
```

Rationale:

Limiting the number of allowed users and sessions per user can limit risks related to denial of service attacks. The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or by a combination thereof.

This requirement addresses concurrent sessions for a single information system account and does not address concurrent sessions by a single user via multiple accounts.

Audit:

Identify the organizational requirements for maximum number of sessions and which users must be restricted. If there are no requirements to limit concurrent sessions, this item does not apply.

For each user requiring concurrent session restrictions, determine if that user is in the user.[username] project where [username] is the user's account username.

projects [username] | grep user

If the output does not include the project user.[username], this is a finding.

Determine the project membership for the user.

projects [username]

If the user is a member of any project other than default, group.[groupname], or user.[username], this is a finding.

Determine whether the max-tasks resource control is enabled properly.

projects -l user.[username] | grep attribs

If the output does not include the text:

attribs: project.max-tasks=(privileged,[MAX],deny)

where [MAX] is the organization-defined maximum number of concurrent sessions, this is a finding.

Remediation:

Identify the organizational requirements for maximum number of sessions and which users must be restricted. If there are no requirements to limit concurrent sessions, this item does not apply.

The Project Management profile is required.

For each user requiring concurrent session restrictions, add the user to the special user.[username] project where [username] is the user's account username where [MAX] is equal to the organizational requirement.

pfexec projadd -K 'project.max-tasks=(privileged,[MAX],deny)' user.[username]

Determine the project membership for the user.

projects [username]

If the user is a member of any projects other than default, group.[groupname], or user.[username], remove that project from the user's account.

The root role is required.

pfedit /etc/user_attr

Locate the line containing the user's username. Remove any project=[projectname] entries from the fifth field.

pfedit /etc/project

Locate the line containing the user's username in a project other than default, group.[groupname], or user.[username], and remove the user from the project's entry or entries from the fourth field.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

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

1.116 SOL-11.1-050010 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must disable directed broadcast packet forwarding.

```
GROUP ID: V-216131
RULE ID: SV-216131r959010
```

Rationale:

This parameter must be disabled to reduce the risk of denial of service attacks.

Audit:

Determine if directed broadcast packet forwarding is disabled.

ipadm show-prop -p _forward_directed_broadcasts -co current ip

If the output of this command is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable directed broadcast packet forwarding.

pfexec ipadm set-prop -p _forward_directed_broadcasts=0 ip

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

1.117 SOL-11.1-050020 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must not respond to ICMP timestamp requests.

```
GROUP ID: V-216132
RULE ID: SV-216132r959010
```

Rationale:

By accurately determining the system's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them.

Audit:

Determine if ICMP time stamp responses are disabled.

ipadm show-prop -p _respond_to_timestamp -co current ip

If the output of both commands is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable source respond to timestamp.

pfexec ipadm set-prop -p _respond_to_timestamp=0 ip

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

1.118 SOL-11.1-050030 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must not respond to ICMP broadcast timestamp requests.

```
GROUP ID: V-216133
RULE ID: SV-216133r959010
```

Rationale:

By accurately determining the system's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them.

Audit:

Determine if response to ICMP broadcast timestamp requests is disabled.

ipadm show-prop -p _respond_to_timestamp_broadcast -co current ip

If the output of this command is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable respond to timestamp broadcasts.

pfexec ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip

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

1.119 SOL-11.1-050040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must not respond to ICMP broadcast netmask requests.

```
GROUP ID: V-216134
RULE ID: SV-216134r959010
```

Rationale:

By determining the netmasks of various computers in your network, an attacker can better map your subnet structure and infer trust relationships.

Audit:

Determine if the response to address mask broadcast is disabled.

ipadm show-prop -p _respond_to_address_mask_broadcast -co current ip

If the output of this command is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable responses to address mask broadcast.

pfexec ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip

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

1.120 SOL-11.1-050050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must not respond to broadcast ICMP echo requests.

```
GROUP ID: V-216135
RULE ID: SV-216135r959010
```

Rationale:

ICMP echo requests can be useful for reconnaissance of systems and for denial of service attacks.

Audit:

Determine if ICMP echo requests response is disabled.

ipadm show-prop -p _respond_to_echo_broadcast -co current ip

If the output of this command is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable respond to echo broadcast.

pfexec ipadm set-prop -p _respond_to_echo_broadcast=0 ip

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

1.121 SOL-11.1-050060 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must not respond to multicast echo requests.

```
GROUP ID: V-216136
RULE ID: SV-216136r959010
```

Rationale:

Multicast echo requests can be useful for reconnaissance of systems and for denial of service attacks.

Audit:

Determine if response to multicast echo requests is disabled.

ipadm show-prop -p _respond_to_echo_multicast -co current ipv4

ipadm show-prop -p _respond_to_echo_multicast -co current ipv6

If the output of all commands is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable respond to echo multi-cast for IPv4 and IPv6.

pfexec ipadm set-prop -p _respond_to_echo_multicast=0 ipv4

pfexec ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

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

1.122 SOL-11.1-050070 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must ignore ICMP redirect messages.

```
GROUP ID: V-216137
RULE ID: SV-216137r959010
```

Rationale:

Ignoring ICMP redirect messages reduces the likelihood of denial of service attacks.

Audit:

Determine if ICMP redirect messages are ignored.

ipadm show-prop -p _ignore_redirect -co current ipv4

ipadm show-prop -p _ignore_redirect -co current ipv6

If the output of all commands is not "1", this is a finding.

Remediation:

The Network Management profile is required.

Disable ignore redirects for IPv4 and IPv6.

pfexec ipadm set-prop -p _ignore_redirect=1 ipv4

pfexec ipadm set-prop -p _ignore_redirect=1 ipv6

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

1.123 SOL-11.1-050080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must set strict multihoming.

```
GROUP ID: V-216138
RULE ID: SV-216138r959010
```

Rationale:

These settings control whether a packet arriving on a non-forwarding interface can be accepted for an IP address that is not explicitly configured on that interface.

This rule is NA for documented systems that have interfaces that cross strict networking domains (for example, a firewall, a router, or a VPN node).

Audit:

Determine if strict multihoming is configured.

ipadm show-prop -p _strict_dst_multihoming -co current ipv4

ipadm show-prop -p _strict_dst_multihoming -co current ipv6

If the output of all commands is not "1", this is a finding.

Remediation:

The Network Management profile is required.

Disable strict multihoming for IPv4 and IPv6.

pfexec ipadm set-prop -p _strict_dst_multihoming=1 ipv4

pfexec ipadm set-prop -p _strict_dst_multihoming=1 ipv6

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

1.124 SOL-11.1-050090 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must disable ICMP redirect messages.

```
GROUP ID: V-216139
RULE ID: SV-216139r959010
```

Rationale:

A malicious user can exploit the ability of the system to send ICMP redirects by continually sending packets to the system, forcing the system to respond with ICMP redirect messages, resulting in an adverse impact on the CPU performance of the system.

Audit:

Determine the version of Solaris 11 in use.

cat /etc/release

If the version of Solaris is earlier than Solaris 11.2, determine if ICMP redirect messages are disabled.

ipadm show-prop -p _send_redirects -co current ipv4

ipadm show-prop -p _send_redirects -co current ipv6

If the output of all commands is not "0", this is a finding.

If the version of Solaris is Solaris 11.2 or later, determine if ICMP redirect messages are disabled.

ipadm show-prop -p send_redirects -co current ipv4

ipadm show-prop -p send_redirects -co current ipv6

If the output of all commands is not "off", this is a finding.

Remediation:

The Network Management profile is required.

If the version of Solaris is earlier than Solaris 11.2, disable send redirects for IPv4 and IPv6.

pfexec ipadm set-prop -p _send_redirects=0 ipv4

pfexec ipadm set-prop -p _send_redirects=0 ipv6

If the version of Solaris is Solaris 11.2 or later, disable send redirects for IPv4 and IPv6.

pfexec ipadm set-prop -p send_redirects=off ipv4

pfexec ipadm set-prop -p send_redirects=off ipv6

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

1.125 SOL-11.1-050100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must disable TCP reverse IP source routing.

```
GROUP ID: V-216140
RULE ID: SV-216140r959010
```

Rationale:

If enabled, reverse IP source routing would allow an attacker to more easily complete a three-way TCP handshake and spoof new connections.

Audit:

Determine if TCP reverse IP source routing is disabled.

ipadm show-prop -p _rev_src_routes -co current tcp

If the output of this command is not "0", this is a finding.

Remediation:

The Network Management profile is required.

Disable reverse source routing.

pfexec ipadm set-prop -p _rev_src_routes=0 tcp

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

1.126 SOL-11.1-050110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must set maximum number of half-open TCP connections to 4096.

```
GROUP ID: V-216141
RULE ID: SV-216141r959010
```

Rationale:

This setting controls how many half-open connections can exist for a TCP port.

It is necessary to control the number of completed connections to the system to provide some protection against denial of service attacks.

Audit:

Determine if the number of half open TCP connections is set to 4096.

ipadm show-prop -p _conn_req_max_q0 -co current tcp

If the value of "4096" is not returned, this is a finding.

Remediation:

The Network Management profile is required

Configure maximum TCP connections for IPv4 and IPv6.

pfexec ipadm set-prop -p _conn_req_max_q0=4096 tcp

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

1.127 SOL-11.1-050120 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must set maximum number of incoming connections to 1024.

```
GROUP ID: V-216142
RULE ID: SV-216142r959010
```

Rationale:

This setting controls the maximum number of incoming connections that can be accepted on a TCP port limiting exposure to denial of service attacks.

Audit:

Determine if the maximum number of incoming connections is set to 1024.

ipadm show-prop -p _conn_req_max_q -co current tcp

If the value returned is smaller than "1024", this is a finding.

In environments where connection numbers are high, such as a busy web server, this value may need to be increased.

Remediation:

The Network Management profile is required.

Configure maximum number of incoming connections.

pfexec ipadm set-prop -p _conn_req_max_q=1024 tcp

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

1.128 SOL-11.1-050130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must disable network routing unless required.

```
GROUP ID: V-216143
RULE ID: SV-216143r959010
```

Rationale:

The network routing daemon, in.routed, manages network routing tables. If enabled, it periodically supplies copies of the system's routing tables to any directly connected hosts and networks and picks up routes supplied to it from other networks and hosts. Routing Internet Protocol (RIP) is a legacy protocol with a number of security weaknesses, including a lack of authentication, zoning, pruning, etc.

Audit:

Determine if routing is disabled.

routeadm -p | egrep "routing |forwarding" | grep enabled

If the command output includes "persistent=enabled" or "current=enabled", this is a finding.

Remediation:

The Network Management profile is required.

Disable routing for IPv4 and IPv6.

pfexec routeadm -d ipv4-forwarding -d ipv4-routing

pfexec routeadm -d ipv6-forwarding -d ipv6-routing

To apply these changes to the running system, use the command:

pfexec routeadm -u

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

1.129 SOL-11.1-050140 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must implement TCP Wrappers.

```
GROUP ID: V-216144
RULE ID: SV-216144r959010
```

Rationale:

TCP Wrappers is a host-based access control system that allows administrators to control who has access to various network services based on the IP address of the remote end of the connection. TCP Wrappers also provides logging information via syslog about both successful and unsuccessful connections.

TCP Wrappers provides granular control over what services can be accessed over the network. Its logs show attempted access to services from non-authorized systems, which can help identify unauthorized access attempts.

Audit:

Determine if TCP Wrappers is configured.

inetadm -p | grep tcp_wrappers

If the output of this command is "FALSE", this is a finding.

The above command will check whether TCP Wrappers is enabled for all TCP-based services started by inetd. TCP Wrappers are enabled by default for sendmail and SunSSH (version 0.5.11). The use of OpenSSH access is controlled by the sshd_config file starting with Solaris

11.3. SunSSH is removed starting with Solaris 11.4.

Individual inetd services may still be configured to use TCP Wrappers even if the global parameter (above) is set to "FALSE". To check the status of individual inetd services, use the command:

for svc in `inetadm | awk '/svc:\// { print $NF }'`; do

val=`inetadm -l ${svc} | grep -c tcp_wrappers=TRUE`

if [${val} -eq 1]; then

echo "TCP Wrappers enabled for ${svc}"

fi

done

If the required services are not configured to use TCP Wrappers, this is finding.

ls /etc/hosts.deny

ls /etc/hosts.allow

If these files are not found, this is a finding.

Remediation:

The root role is required.

Configure allowed and denied hosts per organizational policy.

1. Create and customize the policy in /etc/hosts.allow:

echo "ALL: [net]/[mask] , [net]/[mask], ..." > /etc/hosts.allow
where each [net>/[mask> combination (for example, the Class C address block "192.168.1.0/255.255.255.0") can represent one network block in use by the organization that requires access to this system.

2. Create a default deny policy in /etc/hosts.deny: echo "ALL: ALL" >/etc/hosts.deny
3. Enable TCP Wrappers for all services started by inetd:

inetadm -M tcp_wrappers=TRUE

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

1.130 SOL-11.1-050240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The boundary protection system (firewall) must be configured to deny network traffic by default and must allow network traffic by exception (i.e., deny all, permit by exception).

```
GROUP ID: V-216150
RULE ID: SV-216150r1045457
```

Rationale:

A firewall that relies on a deny all, permit by exception strategy requires all traffic to have explicit permission before traversing an interface on the host. The firewall must incorporate stateful packet filtering and logging.

Nonlocal maintenance and diagnostic communications often contain sensitive information and must be protected. The security of these remote accesses can be ensured by sending nonlocal maintenance and diagnostic communications through encrypted channels enforced via firewall configurations.

Satisfies: SRG-OS-000074, SRG-OS-000096, SRG-OS-000112, SRG-OS-000113, SRG-OS-000125, SRG-OS-000250, SRG-OS-000393

Audit:

Ensure that either the IP Filter or Packet Filter Firewall is installed correctly.

Determine the OS version to be secured.

uname -v

For Solaris 11, 11.1, 11.2, and 11.3, which use IP Filter, the IP Filter Management profile is required.

Check that the IP Filter firewall is enabled and configured so that only authorized sessions are allowed.

svcs ipfilter

If "ipfilter" is not listed with a state of "online", this is a finding.

The IP Filter Management profile is required.

Check that the filters are configured properly.

ipfstat -io

If the output of this command does not include the following lines, this is a finding.

block out log all keep state keep frags

block in log all

block in log from any to 255.255.255.255/32

block in log from any to 127.0.0.1/32

Even if the lines above are included in the output, it is possible that other lines can contradict the firewall settings. Review the firewall rules and ensure that they conform to organizational and mission requirements. If the firewall rules are not configured to organizational standards, this is a finding.

For Solaris 11.3 or newer, which use Packet Filter, the Network Firewall Management rights profile is required.

Check that the Packet Filter firewall is enabled and configured so that only authorized sessions are allowed.

svcs firewall:default

If "firewall" is not listed with a state of "online", this is a finding.

The Network Firewall Management rights profile is required.

Check that the filters are configured properly.

pfctl -s rules

If the output of this command does not include a line to block and log all traffic as in the following line, this is a finding (does not have to be exactly like the example).

block drop log (to pflog0) all

Check that the Packet Filter firewall logging daemon is enabled.

svcs firewall/pflog:default

If "pflog" is not listed with a state of "online", this is a finding.

Remediation:

The root role is required.

For Solaris 11, 11.1, 11.2, and 11.3, which use IP Filter, configure and enable the IP Filters policy.

pfedit /etc/ipf/ipf.conf.

Add the following lines to the file:

Do not allow all outbound traffic, keep state, and log

block out log all keep state keep frags

Block and log everything else that comes in

block in log all

block in log from any to 255.255.255.255

block in log from any to 127.0.0.1/32

Enable ipfilter.

svcadm enable ipfilter

Notify ipfilter to use the new configuration file.

ipf -Fa -f /etc/ipf/ipf.conf

For Solaris 11.3 or newer, which use Packet Filter, configure and enable the Packet Filter’s policy.

pfedit /etc/firewall/pf.conf.

Add either of the following lines to the file:

Block and log all traffic on all interfaces in either direction from anywhere to anywhere

block log all

-or-

Drop traffic and log it to a fllog interface for more detailed inspection or analysis using tools like tcpdump

block drop log (to pflog0) all

Enable Packet Filter.

svcadm enable firewall:default

Enable Packet Filter logging daemon.

svcadm enable firewall/pflog:default

Note: Because the default firewall rules block all network access to the system, ensure there is still a method to access the system, such as SSH or console access, prior to activating the firewall rules. Operational requirements may dictate the addition of protocols such as SSH, DNS, NTP, HTTP, and HTTPS to be allowed.

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-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

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-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

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-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-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-001942 The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (9)

1.131 SOL-11.1-050370 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must prevent local applications from generating source-routed packets.

```
GROUP ID: V-216157
RULE ID: SV-216157r959010
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.

Audit:

Determine the OS version you are currently securing.

uname –v

Solaris 11, 11.1, 11.2, and 11.3 use IP Filter. To continue checking IP Filter, the IP Filter Management profile is required.

Check the system for an IPF rule blocking outgoing source-routed packets.

ipfstat -o

Examine the list for rules such as:

block out log quick from any to any with opt lsrr

block out log quick from any to any with opt ssrr

If the listed rules do not block both lsrr and ssrr options, this is a finding.

For Solaris 11.3 or newer that use Packet Filter, the Network Firewall Management rights profile is required.

Ensure that IP Options are not in use:

pfctl -s rules | grep allow-opts

If any output is returned, this is a finding.

Remediation:

The root role is required.

pfedit /etc/ipf/ipf.conf

For Solaris 11, 11.1, 11.2, and 11.3 that use IP Filter dd rules to block outgoing source-routed packets, such as:

block out log quick all with opt lsrr

block out log quick all with opt ssrr

Reload the IPF rules.

ipf -Fa -A -f /etc/ipf/ipf.conf

For Solaris 11.3 or newer that use Packet Filter remove or modify any rules that include "allow-opts".

Reload the Packet Filter rules:

svcadm refresh firewall:default

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

1.132 SOL-11.1-050380 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must display the DoD approved system use notification message or banner before granting access to the system for general system logons.

```
GROUP ID: V-216158
RULE ID: SV-216158r958390
```

Rationale:

Warning messages inform users who are attempting to log in to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. As implementing a logon banner to deter inappropriate use can provide a foundation for legal action against abuse, this warning content should be set as appropriate.

Audit:

Review the contents of these two files and check that the proper DoD banner message is configured.

cat /etc/motd

cat /etc/issue

If the DoD-approved banner text is not in the files, this is a finding.

Remediation:

The root role is required.

Edit the contents of these two files and ensure that the proper DoD banner message is viewable.

pfedit /etc/motd

pfedit /etc/issue

The DoD required text is:

"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."

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

1.133 SOL-11.1-050390 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must display the DoD approved system use notification message or banner for SSH connections.

```
GROUP ID: V-216159
RULE ID: SV-216159r958390
```

Rationale:

Warning messages inform users who are attempting to log in to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. As implementing a logon banner to deter inappropriate use can provide a foundation for legal action against abuse, this warning content should be set as appropriate.

Audit:

Check SSH configuration for banner message:

grep "^Banner" /etc/ssh/sshd_config

If the output is not:

Banner /etc/issue

and /etc/issue does not contain the approved banner text, this is a finding.

Remediation:

The root role is required.

Edit the SSH configuration file.

pfedit /etc/ssh/sshd_config

Locate the file containing:

Banner

Change the line to read:

Banner /etc/issue

Edit the /etc/issue file

pfedit /etc/issue

The DoD required text is:

"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."

Restart the SSH service

svcadm restart svc:/network/ssh

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

1.134 SOL-11.1-050410 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The GNOME service must display the DoD approved system use notification message or banner before granting access to the system.

```
GROUP ID: V-216160
RULE ID: SV-216160r958390
```

Rationale:

Warning messages inform users who are attempting to log in to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. As implementing a logon banner to deter inappropriate use can provide a foundation for legal action against abuse, this warning content should be set as appropriate.

Audit:

This item does not apply if a graphic login is not configured.

Log in to the Gnome Graphical interface. If the approved banner message does not appear, this is a finding.

cat /etc/issue

grep /etc/gdm/Init/Default zenity

If /etc/issue does not contain that DoD-approved banner message or /etc/gdm/Init/Default does not contain the line:

/usr/bin/zenity --text-info --width=800 --height=300

--title="Security Message" --filename=/etc/issue

this is a finding.

Remediation:

The root role is required.

If the system does not use XWindows, this is not applicable.

pfedit /etc/issue

Insert the proper DoD banner message text. The DoD required text is:

"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."

pfedit /etc/gdm/Init/Default

Add the following content before the "exit 0" line of the file.

/usr/bin/zenity --text-info --width=800 --height=300

--title="Security Message" --filename=/etc/issue

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

1.135 SOL-11.1-050430 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The FTP service must display the DoD approved system use notification message or banner before granting access to the system.

```
GROUP ID: V-216161
RULE ID: SV-216161r958390
```

Rationale:

Warning messages inform users who are attempting to log in to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. As implementing a logon banner to deter inappropriate use can provide a foundation for legal action against abuse, this warning content should be set as appropriate.

Audit:

Determine if the FTP server package is installed:

pkg list service/network/ftp

If the package is not installed, this check does not apply.

grep DisplayConnect /etc/proftpd.conf

If:

DisplayConnect /etc/issue

does not appear, this is a finding.

If /etc/issue does not contain the approved DoD text, this is a finding.

Remediation:

The root role is required.

The package: pkg:/service/network/ftp must be installed.

pfedit /etc/issue

Insert the proper DoD banner message text. The DoD required text is:

"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."

echo "DisplayConnect /etc/issue" >> /etc/proftpd.conf

svcadm restart ftp

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

1.136 SOL-11.1-050460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must terminate all sessions and network connections when nonlocal maintenance is completed.

```
GROUP ID: V-216162
RULE ID: SV-216162r986457
```

Rationale:

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

The operating system needs to ensure all sessions and network connections are terminated when nonlocal maintenance is completed.

Audit:

Determine if SSH is configured to disconnect sessions after 10 minutes of inactivity.

grep ClientAlive /etc/ssh/sshd_config

If the output of this command is not as shown below, this is a finding.

ClientAliveInterval 600

ClientAliveCountMax 0

Remediation:

The root role is required.

Configure the system to disconnect SSH sessions after 10 minutes of inactivity.

pfedit /etc/ssh/sshd_config

Insert the two lines:

ClientAliveInterval 600

ClientAliveCountMax 0

Restart the SSH service with the new configuration.

svcadm restart svc:/network/ssh

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

1.137 SOL-11.1-050470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent internal users from sending out packets which attempt to manipulate or spoof invalid IP addresses.

```
GROUP ID: V-216163
RULE ID: SV-216163r959010
```

Rationale:

Manipulation of IP addresses can allow untrusted systems to appear as trusted hosts, bypassing firewall and other security mechanism and resulting in system penetration.

Audit:

Determine the zone that you are currently securing.

zonename

If the command output is "global", then only the "phys" and "SR-IOV" interfaces assigned to the global zone require inspection. If using a non-Global zone, then all "phys" and "SR-IOV" interfaces assigned to the zone require inspection.

Identify if this system has physical interfaces.

dladm show-link -Z | grep -v vnic

LINK ZONE CLASS MTU STATE OVER

net0 global phys 1500 unknown --

e1000g0 global phys 1500 up --

e1000g1 global phys 1500 up --

zoneD/net2 zoneD iptun 65515 up --

If "phys" appears in the third column, then the interface is physical.

For each physical interface, determine if the network interface is Ethernet or InfiniBand:

dladm show-phys [interface name]

LINK MEDIA STATE SPEED DUPLEX DEVICE

[name] Ethernet unknown 0 half dnet0

The second column indicates either "Ethernet" or "Infiniband".

For each physical interface, determine if the host is using ip-forwarding:

ipadm show-ifprop [interface name] | grep forwarding

[name] forwarding ipv4 rw off -- off on,off

[name] forwarding ipv6 rw off -- off on,off

If "on" appears in the fifth column, then the interface is using ip-forwarding.

For each interface, determine if the host is using SR-IOV’s Virtual Function (VF) driver:

dladm show-phys [interface name] | grep vf

If the sixth column includes 'vf' in its name, it is using SR-IOV (ex: ixgbevf0).

For each physical and SR-IOV interface, determine if network link protection capabilities are enabled.

dladm show-linkprop -p protection

LINK PROPERTY PERM VALUE DEFAULT POSSIBLE

net0 protection rw mac-nospoof, -- mac-nospoof,

restricted, restricted,

ip-nospoof, ip-nospoof,

dhcp-nospoof dhcp-nospoof

If the interface uses Infiniband and if restricted, ip-nospoof, and dhcp-nospoof do not appear in the "VALUE" column, this is a finding.

If the interface uses ip-forwarding and if mac-nospoof, restricted, and dhcp-nospoof do not appear in the "VALUE" column, this is a finding.

If the interface uses SR-IOV and if mac-nospoof, restricted, and dhcp-nospoof do not appear in the "VALUE" column, this is a finding.

If the interface uses Ethernet without IP forwarding and if mac-nospoof, restricted, ip-nospoof, and dhcp-nospoof do not appear in the "VALUE" column, this is a finding.

Remediation:

Determine the name of the zone that you are currently securing.

zonename

If the command output is "global", then only the "phys" and "SR-IOV" interfaces assigned to the global zone require configuration. If using a non-Global zone, then all "phys" and "SR-IOV" interfaces assigned to the zone require configuration.

The Network Link Security profile is required.

Determine which network interfaces are available and what protection modes are enabled and required.

Enable link protection based on each configured network interface type.

For InfiniBand:

pfexec dladm set-linkprop -p protection=restricted,ip-nospoof,dhcp-nospoof [interface name]

For IP forwarding:

pfexec dladm set-linkprop -p protection=mac-nospoof,restricted,dhcp-nospoof [interface name]

For SR-IOV:

pfexec dladm set-linkprop -p protection=mac-nospoof,restricted,dhcp-nospoof [interface name]

For Ethernet without IP forwarding:

pfexec dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof [interface name]

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

1.138 SOL-11.1-050480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Wireless network adapters must be disabled.

```
GROUP ID: V-216164
RULE ID: SV-216164r958358
```

Rationale:

The use of wireless networking can introduce many different attack vectors into the organization’s network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack or be used to create a denial-of-service to valid network resources.

Audit:

This is N/A for systems that do not have wireless network adapters.

Verify that there are no wireless interfaces configured on the system:

ifconfig -a

eth0 Link encap:Ethernet HWaddr b8:ac:6f:65:31:e5

inet addr:192.168.2.100 Bcast:192.168.2.255 Mask:255.255.255.0

inet6 addr: fe80::baac:6fff:fe65:31e5/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:2697529 errors:0 dropped:0 overruns:0 frame:0

TX packets:2630541 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:2159382827 (2.0 GiB) TX bytes:1389552776 (1.2 GiB)

Interrupt:17

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:2849 errors:0 dropped:0 overruns:0 frame:0

TX packets:2849 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:2778290 (2.6 MiB) TX bytes:2778290 (2.6 MiB)

If a wireless interface is configured, it must be documented and approved by the local Authorizing Official.

If a wireless interface is configured and has not been documented and approved, this is a finding.

Remediation:

Configure the system to disable all wireless network interfaces.

Additional Information:

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)

CCI-001444 Protect wireless access to the system using encryption.

- 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)

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

1.139 SOL-11.1-060010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must use mechanisms for authentication to a cryptographic module meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for such authentication.

```
GROUP ID: V-216165
RULE ID: SV-216165r958358
```

Rationale:

Encryption is only as good as the encryption modules utilized. Unapproved cryptographic module algorithms cannot be verified, and cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised due to weak algorithms.

Applications utilizing encryption are required to use approved encryption modules meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance.

FIPS 140-2 is the current standard for validating cryptographic modules, and NSA Type-X (where X=1, 2, 3, 4) products are NSA-certified hardware based encryption modules.

Satisfies: SRG-OS-000120, SRG-OS-000169

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The Crypto Management profile is required to execute this command.

Check to ensure that FIPS-140 encryption mode is enabled.

cryptoadm list fips-140| grep -c "is disabled"

If the output of this command is not "0", this is a finding.

Remediation:

The Crypto Management profile is required to execute this command.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Enable FIPS-140 mode.

pfexec cryptoadm enable fips-140

Reboot the system as requested.

Additional Information:

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

1.140 SOL-11.1-060060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ FIPS-validate or NSA-approved cryptography to implement digital signatures.

```
GROUP ID: V-220003
RULE ID: SV-220003r987791
```

Rationale:

FIPS 140-2 is the current standard for validating cryptographic modules, and NSA Type-X (where X=1, 2, 3, 4) products are NSA-certified hardware based encryption modules.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The Crypto Management profile is required to execute this command.

Check to ensure that FIPS-140 encryption mode is enabled.

cryptoadm list fips-140| grep -c "is disabled"

If the output of this command is not "0", this is a finding.

Remediation:

The Crypto Management profile is required to execute this command.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Enable FIPS-140 mode.

pfexec cryptoadm enable fips-140

Reboot the system as requested.

Additional Information:

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

1.141 SOL-11.1-060070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect the integrity of transmitted information.

```
GROUP ID: V-220004
RULE ID: SV-220004r958908
```

Rationale:

Ensuring the integrity of transmitted information requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

All remote sessions must be conducted via encrypted services and ports.

Check that SSH is enabled:

svcs svc:/network/ssh

STATE STIME FMRI

online Nov_03 svc:/network/ssh:default

Ask the operator to document all configured external ports and protocols.

If any unencrypted connections are used, this is a finding.

Remediation:

Configure SSH to be enabled.

svcadm enable svc:/network/ssh

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

1.142 SOL-11.1-060080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

```
GROUP ID: V-220005
RULE ID: SV-220005r971547
```

Rationale:

Ensuring that transmitted information is not altered during transmission requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

All remote sessions must be conducted via encrypted services and ports.

Check that SSH is enabled:

svcs svc:/network/ssh

STATE STIME FMRI

online Nov_03 svc:/network/ssh:default

Ask the operator to document all configured external ports and protocols.

If any unencrypted connections are used, this is a finding.

Remediation:

Configure SSH to be enabled.

svcadm enable svc:/network/ssh

Additional Information:

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)

1.143 SOL-11.1-060090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must maintain the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

```
GROUP ID: V-220006
RULE ID: SV-220006r958912
```

Rationale:

Ensuring the integrity of transmitted information requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

All remote sessions must be conducted via encrypted services and ports.

Ask the operator to document all configured external ports and protocols. If any unencrypted connections are used, this is a finding.

Remediation:

All remote sessions must be conducted via SSH and IPsec. Ensure that SSH and IPsec are the only protocols used.

Additional Information:

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

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

1.144 SOL-11.1-060100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect the confidentiality of transmitted information.

```
GROUP ID: V-220007
RULE ID: SV-220007r958908
```

Rationale:

Ensuring the confidentiality of transmitted information requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

All remote sessions must be conducted via encrypted services and ports.

Ask the operator to document all configured external ports and protocols. If any unencrypted connections are used, this is a finding.

Remediation:

All remote sessions must be conducted via SSH and IPsec. Ensure that SSH and IPsec are the only protocols used.

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

1.145 SOL-11.1-060110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

```
GROUP ID: V-220008
RULE ID: SV-220008r971547
```

Rationale:

Ensuring that transmitted information does not become disclosed to unauthorized entities requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

All remote sessions must be conducted via encrypted services and ports.

Ask the operator to document all configured external ports and protocols. If any unencrypted connections are used, this is a finding.

Remediation:

All remote sessions must be conducted via SSH and IPsec. Ensure that SSH and IPsec are the only protocols used.

Additional Information:

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)

1.146 SOL-11.1-060120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must maintain the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

```
GROUP ID: V-220009
RULE ID: SV-220009r958912
```

Rationale:

Ensuring that transmitted information remains confidential during aggregation, packaging, and transformation requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

All remote sessions must be conducted via encrypted services and ports.

Ask the operator to document all configured external ports and protocols. If any unencrypted connections are used, this is a finding.

Remediation:

All remote sessions must be conducted via SSH and IPsec. Ensure that SSH and IPsec are the only protocols used.

Additional Information:

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

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

1.147 SOL-11.1-060130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement DoD-approved encryption to protect the confidentiality of remote access sessions.

```
GROUP ID: V-216173
RULE ID: SV-216173r958408
```

Rationale:

Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless.

Using cryptography ensures confidentiality of the remote access connections.

The system will attempt to use the first cipher presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest cipher available to secure the SSH connection.

Note: SSH in Solaris 11.GA-11.3 used Sun Microsystem’s proprietary SUNWssh. In Solaris 11.3 OpenSSH was offered as optional software and in Solaris 11.4 OpenSSH is the only SSH offered. Both use the same /etc/ssh/sshd_config file and both, by default do not include the ciphers line.

Audit:

Check the SSH daemon configuration for allowed ciphers.

grep -i ciphers /etc/ssh/sshd_config | grep -v '^#’

Ciphers aes256-ctr,aes192-ctr,aes128-ctr

If any ciphers other than "aes256-ctr", "aes192-ctr", or "aes128-ctr" are listed, the order differs from the example above, the "Ciphers" keyword is missing, or is commented out, this is a finding.

Remediation:

The root role is required.

Modify the sshd_config file.

pfedit /etc/ssh/sshd_config

Change or set the ciphers line to the following:

ciphers aes256-ctr,aes192-ctr,aes128-ctr

Restart the SSH service.

svcadm restart svc:/network/ssh

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)

1.148 SOL-11.1-060140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must use cryptographic mechanisms to protect and restrict access to information on portable digital media.

```
GROUP ID: V-216174
RULE ID: SV-216174r959010
```

Rationale:

When data is written to portable digital media, such as thumb drives, floppy diskettes, compact disks, and magnetic tape, etc., there is risk of data loss.

An organizational assessment of risk guides the selection of media and associated information contained on the media requiring restricted access.

Organizations need to document in policy and procedures the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel.

In these situations, it is assumed the physical access controls where the media resides provide adequate protection. The employment of cryptography is at the discretion of the information owner/steward.

When the organization has determined the risk warrants it, data written to portable digital media must be encrypted.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the logical node of all attached removable media:

rmformat

This command lists all attached removable devices. Note the device logical node name. For example: /dev/rdsk/c8t0d0p0

Determine which zpool is mapped to the device:

zpool status

Determine the file system names of the portable digital media:

zfs list | grep [poolname]

Using the file system name, determine if the removal media is encrypted:

zfs get encryption [filesystem]

If "encryption off" is listed, this is a finding.

Remediation:

The root role is required.

Format a removable device as a ZFS encrypted file system.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

The ZFS File System Management and ZFS Storage management profiles are required.

Insert the removable device:

rmformat

This command lists all attached removable devices. Note the device logical node name. For example: /dev/rdsk/c8t0d0p0

Create an encrypted zpool on this device using a poolname of your choice:

pfexec zpool create -O encryption=on [poolname] c8t0d0p0

Enter a passphrase and confirm the passphrase. Keep the passphrase secure.

Export the zpool before removing the media:

pfexec export [poolname]

It will be necessary to enter the passphrase when inserting and importing the removable media zpool:

Insert the removable media

pfexec import [poolname]

Only store data in the encrypted file system.

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

1.149 SOL-11.1-060150 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must employ cryptographic mechanisms to protect information in storage.

```
GROUP ID: V-220010
RULE ID: SV-220010r958870
```

Rationale:

When data is written to digital media, such as hard drives, mobile computers, external/removable hard drives, personal digital assistants, flash/thumb drives, etc., there is risk of data loss and data compromise.

An organizational assessment of risk guides the selection of media and associated information contained on the media requiring restricted access. Organizations need to document in policy and procedures the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed the physical access controls where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information.

Audit:

Determine if file system encryption is required by your organization. If not required, this item does not apply.

Determine if file system encryption is enabled for user data sets. This check does not apply to the root, var, share, swap or dump datasets.

zfs list

Using the file system name, determine if the file system is encrypted:

zfs get encryption [filesystem]

If "encryption off" is listed, this is a finding.

Remediation:

The ZFS file system management profile is required.

ZFS file system encryption may only be enabled on creation of the file system. If a file system must be encrypted and is not, its data should be archived, it must be removed and re-created.

First, stop running applications using the file systems, archive the data, unmount, and then remove the file system.

umount [file system name]

zfs destroy [file system name]

When creating ZFS file systems, ensure that they are created as encrypted file systems.

pfexec zfs create -o encryption=on [file system name]

Enter passphrase for '[file system name]': xxxxxxx

Enter again: xxxxxxx

Store the passphrase in a safe location. The passphrase will be required to mount the file systems upon system reboot. If automated mounting is required, the passphrase must be stored in a file.

Additional Information:

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)

1.150 SOL-11.1-060160 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must protect the confidentiality and integrity of information at rest.

```
GROUP ID: V-216176
RULE ID: SV-216176r958552
```

Rationale:

When data is written to digital media, such as hard drives, mobile computers, external/removable hard drives, personal digital assistants, flash/thumb drives, etc., there is risk of data loss and data compromise.

An organizational assessment of risk guides the selection of media and associated information contained on the media requiring restricted access. Organizations need to document in policy and procedures the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed the physical access controls where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information.

Audit:

Determine if file system encryption is required by your organization. If not required, this item does not apply.

Determine if file system encryption is enabled for user data sets. This check does not apply to the root, var, share, swap or dump datasets.

zfs list

Using the file system name, determine if the file system is encrypted:

zfs get encryption [filesystem]

If "encryption off" is listed, this is a finding.

Remediation:

The ZFS file system management profile is required.

ZFS file system encryption may only be enabled on creation of the file system. If a file system must be encrypted and is not, its data should be archived, it must be removed and re-created.

First, stop running applications using the file systems, archive the data, unmount, and then remove the file system.

umount [file system name]

zfs destroy [file system name]

When creating ZFS file systems, ensure that they are created as encrypted file systems.

pfexec zfs create -o encryption=on [file system name]

Enter passphrase for '[file system name]': xxxxxxx

Enter again: xxxxxxx

Store the passphrase in a safe location. The passphrase will be required to mount the file systems upon system reboot. If automated mounting is required, the passphrase must be stored in a file.

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

1.151 SOL-11.1-060170 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must employ cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures.

```
GROUP ID: V-220011
RULE ID: SV-220011r958870
```

Rationale:

When data is written to digital media, such as hard drives, mobile computers, external/removable hard drives, personal digital assistants, flash/thumb drives, etc., there is risk of data loss and data compromise.

An organizational assessment of risk guides the selection of media and associated information contained on the media requiring restricted access. Organizations need to document in policy and procedures the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed the physical access controls where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information.

Audit:

Determine if file system encryption is required by your organization. If not required, this item does not apply.

Determine if file system encryption is enabled for user data sets. This check does not apply to the root, var, share, swap or dump datasets.

zfs list

Using the file system name, determine if the file system is encrypted:

zfs get encryption [filesystem]

If "encryption off" is listed, this is a finding.

Remediation:

The ZFS file system management profile is required.

ZFS file system encryption may only be enabled on creation of the file system. If a file system must be encrypted and is not, its data should be archived, it must be removed and re-created.

First, stop running applications using the file systems, archive the data, unmount, and then remove the file system.

umount [file system name]

zfs destroy [file system name]

When creating ZFS file systems, ensure that they are created as encrypted file systems.

pfexec zfs create -o encryption=on [file system name]

Enter passphrase for '[file system name]': xxxxxxx

Enter again: xxxxxxx

Store the passphrase in a safe location. The passphrase will be required to mount the file systems upon system reboot. If automated mounting is required, the passphrase must be stored in a file.

Additional Information:

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)

1.152 SOL-11.1-060180 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must use cryptographic mechanisms to protect the integrity of audit information.

```
GROUP ID: V-216178
RULE ID: SV-216178r958576
```

Rationale:

Protection of audit records and audit data is of critical importance. Cryptographic mechanisms are the industry established standard used to protect the integrity of audit data.

Audit:

The Audit Configuration and the Audit Control profiles are required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine if audit log encryption is required by your organization. If not required, this check does not apply.

Determine where the audit logs are stored and whether the file system is encrypted.

pfexec auditconfig -getplugin audit_binfile

The p_dir attribute lists the location of the audit log filesystem.

The default location for Solaris 11.1 is /var/audit. /var/audit is a link to /var/share/audit which, by default, is mounted on rpool/VARSHARE.

Determine if this is encrypted:

zfs get encryption rpool/VARSHARE

If the file system where audit logs are stored reports "encryption off", this is a finding.

Remediation:

The ZFS File System Management and ZFS Storage Management profiles are required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

The Audit Configuration and the Audit Control profiles are required.

If necessary, create a new ZFS pool to store the encrypted audit logs.

pfexec zpool create auditp mirror [device] [device]

Create an encryption key:

pktool genkey keystore=file outkey=/[filename] keytype=aes keylen=256

Create a new file system to store the audit logs with encryption enabled. Use the file name created in the previous step as the keystore.

pfexec zfs create -o encryption=aes-256-ccm -o keysource=raw,file:///[filename] -o compression=on -o mountpoint=/audit auditp/auditf

Configure auditing to use this encrypted directory.

pfexec auditconfig -setplugin audit_binfile p_dir=/audit/

Refresh the audit service for the setting to be applied:

pfexec audit -s

Additional Information:

CCI-001350 Implement cryptographic mechanisms to protect the integrity of audit information.

- 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)

1.153 SOL-11.1-060190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect the integrity of transmitted information.

```
GROUP ID: V-220012
RULE ID: SV-220012r958908
```

Rationale:

Ensuring the integrity of transmitted information requires the operating system take feasible measures to employ transmission layer security. This requirement applies to communications across internal and external networks.

Audit:

The operator shall determine if IPsec is being used to encrypt data for activities such as cluster interconnects or other non-SSH, SFTP data connections.

On both systems review the file /etc/inet/ipsecinit.conf. Ensure that connections between hosts are configured properly in this file per the Solaris 11 documentation.

Check that the IPsec policy service is online:

svcs svc:/network/ipsec/policy:default

If the IPsec service is not online, this is a finding.

If encrypted protocols are not used between systems, this is a finding.

Remediation:

The Service Management profile is required.

Configure IPsec encrypted tunneling between two systems.

On both systems review the file /etc/inet/ipsecinit.conf. Ensure that connections between hosts are configured properly in this file per the Solaris 11 documentation.

Ensure that the IPsec policy service is online:

Enable the IPsec service:

svcadm enable svc:/network/ipsec/policy:default

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

1.154 SOL-11.1-070010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The sticky bit must be set on all world writable directories.

```
GROUP ID: V-216180
RULE ID: SV-216180r959010
```

Rationale:

Files in directories that have had the "sticky bit" enabled can only be deleted by users that have both write permissions for the directory in which the file resides, as well as ownership of the file or directory, or have sufficient privileges. As this prevents users from overwriting each others' files, whether it be accidental or malicious, it is generally appropriate for most world-writable directories (e.g., /tmp).

Audit:

The root role is required.

Identify all world-writable directories without the "sticky bit" set.

find / (-fstype nfs -o -fstype cachefs -o -fstype autofs

-o -fstype ctfs -o -fstype mntfs -o -fstype objfs

-o -fstype proc) -prune -o -type d (-perm -0002

-a ! -perm -1000) -ls

Output of this command identifies world-writable directories without the "sticky bit" set. If output is created, this is a finding.

Remediation:

The root role is required.

Ensure that the "sticky bit" is set on any directories identified during the check steps.

chmod +t [directory name]

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

1.155 SOL-11.1-070020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Permissions on user home directories must be 750 or less permissive.

```
GROUP ID: V-216181
RULE ID: SV-216181r959010
```

Rationale:

Group-writable or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

The root role is required.

Check that the permissions on users' home directories are 750 or less permissive.

for dir in `logins -ox |\ awk -F: '($8 == "PS") { print $6 }'`; do

find ${dir} -type d -prune (-perm -g+w -o

-perm -o+r -o -perm -o+w -o -perm -o+x) -ls

done

If output is created, this is finding.

Remediation:

The root role is required.

Change the permissions on users' directories to 750 or less permissive.

chmod 750 [directory name]

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

1.156 SOL-11.1-070030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Permissions on user . (hidden) files must be 750 or less permissive.

```
GROUP ID: V-216182
RULE ID: SV-216182r959010
```

Rationale:

Group-writable or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

The root role is required.

Ensure that the permissions on user "." files are 750 or less permissive.

for dir in

logins -ox | awk -F: '($8 == "PS") { print $6 }'; do

find ${dir}/.[A-Za-z0-9]* ! -type l

(-perm -0001 -o -perm -0002 -o -perm -0004 -o -perm -0020) -ls

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Change the permissions on users' "." files to 750 or less permissive.

chmod 750 [file name]

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

1.157 SOL-11.1-070040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Permissions on user .netrc files must be 750 or less permissive.

```
GROUP ID: V-216183
RULE ID: SV-216183r959010
```

Rationale:

.netrc files may contain unencrypted passwords that can be used to attack other systems.

Audit:

The root role is required.

Check that permissions on user .netrc files are 750 or less permissive.

for dir in

logins -ox | awk -F: '($8 == "PS") { print $6 }'; do

find ${dir}/.netrc -type f (

-perm -g+r -o -perm -g+w -o -perm -g+x -o

-perm -o+r -o -perm -o+w -o -perm -o+x)

-ls 2>/dev/null

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Change the permissions on users' .netrc files to 750 or less permissive.

chmod 750 [file name]

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

1.158 SOL-11.1-070050 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no user .rhosts files.

```
GROUP ID: V-216184
RULE ID: SV-216184r959010
```

Rationale:

Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

The root role is required.

Check for the presence of .rhosts files.

for dir in

logins -ox | awk -F: '($8 == "PS") { print $6 }'; do

find ${dir}/.rhosts -type f -ls 2>/dev/null

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Remove any .rhosts files found.

rm [file name]

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

1.159 SOL-11.1-070060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Groups assigned to users must exist in the /etc/group file.

```
GROUP ID: V-216185
RULE ID: SV-216185r959010
```

Rationale:

Groups defined in passwd but not in group file pose a threat to system security since group permissions are not properly managed.

Audit:

The root role is required.

Check that groups are configured correctly.

logins -xo | awk -F: '($3 == "") { print $1 }'

If output is produced, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the Audit step. Determine if any groups are in passwd but not in group, and work with those users or group owners to determine the best course of action in accordance with site policy.

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

1.160 SOL-11.1-070070 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Users must have a valid home directory assignment.

```
GROUP ID: V-216186
RULE ID: SV-216186r959010
```

Rationale:

All users must be assigned a home directory in the passwd file. Failure to have a home directory may result in the user being put in the root directory.

Audit:

The root role is required.

Determine if each user has a valid home directory.

logins -xo | while read line; do

user=echo ${line} | awk -F: '{ print $1 }'

home=echo ${line} | awk -F: '{ print $6 }'

if [-z "${home}"]; then

echo ${user}

fi

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the check step. Determine if there exists any users who are in passwd but do not have a home directory, and work with those users to determine the best course of action in accordance with site policy. This generally means deleting the user or creating a valid home directory.

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

1.161 SOL-11.1-070080 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

All user accounts must be configured to use a home directory that exists.

```
GROUP ID: V-216187
RULE ID: SV-216187r959010
```

Rationale:

If the user's home directory does not exist, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

The root role is required.

Check if a GUI is installed.

Determine the OS version you are currently securing:.

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

pkg info gdm

pkg info coherence-26

pkg info coherence-27

If none of these packages are installed on the system, then no GUI is present.

For Solaris 11.4 or newer:

pkg info gdm

If gdm is not installed on the system, then no GUI is present.

pkg info uucp

uucp is no longer installed by default starting in 11.4 and is deprecated.

For all versions, check that all users' home directories exist.

pwck

Accounts with no home directory will output "Login directory not found".

If no GUI is present, then "gdm" and "upnp" accounts should generate errors. On all systems, with uucp package installed, the "uucp" and "nuucp" accounts should generate errors.

If users' home directories do not exist, this is a finding.

Remediation:

The root role is required.

Work with users identified in the check step to determine the best course of action in accordance with site policy. This generally means deleting the user account or creating a valid home directory.

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

1.162 SOL-11.1-070090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All home directories must be owned by the respective user assigned to it in /etc/passwd.

```
GROUP ID: V-216188
RULE ID: SV-216188r959010
```

Rationale:

Since the user is accountable for files stored in the user's home directory, the user must be the owner of the directory.

Audit:

The root role is required.

Check that home directories are owned by the correct user.

export IFS=":"; logins -uxo | while read user uid group gid gecos home rest; do result=$(find ${home} -type d -prune ! -user $user -print 2>/dev/null);

if [! -z "${result}"]; then

echo "User: ${user}\tOwner: $(ls -ld $home | awk '{ print $3 }')";

fi;

done

If any output is produced, this is a finding.

Remediation:

The root role is required.

Correct the owner of any directory that does not match the password file entry for that user.

chown [user] [home directory]

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

1.163 SOL-11.1-070100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Duplicate User IDs (UIDs) must not exist for users within the organization.

```
GROUP ID: V-216189
RULE ID: SV-216189r958482
```

Rationale:

Users within the organization must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

The root role is required.

Check that there are no duplicate UIDs.

logins -d

If output is produced, this is a finding.

Remediation:

The root role is required.

Determine if there exists any users who share a common UID, and work with those users to determine the best course of action in accordance with site policy.

Change user account names and UID or delete accounts, so each account has a unique name and UID.

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

1.164 SOL-11.1-070110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Duplicate UIDs must not exist for multiple non-organizational users.

```
GROUP ID: V-216190
RULE ID: SV-216190r958504
```

Rationale:

Non-organizational users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

The root role is required.

Check that there are no duplicate UIDs.

logins -d

If output is produced, this is a finding.

Remediation:

The root role is required.

Determine if there exists any users who share a common UID, and work with those users to determine the best course of action in accordance with site policy.

Change user account names and UID or delete accounts, so each account has a unique name and UID.

Additional Information:

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

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

1.165 SOL-11.1-070120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Duplicate Group IDs (GIDs) must not exist for multiple groups.

```
GROUP ID: V-216191
RULE ID: SV-216191r959010
```

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

The root role is required.

Check that group IDs are unique.

getent group | cut -f3 -d":" | sort -n | uniq -c |

while read x ; do

[-z "${x}"] && break

set - $x

if [$1 -gt 1]; then

grps=getent group | nawk -F: '($3 == n) { print $1 }' n=$2 | xargs

echo "Duplicate GID ($2): ${grps}"

fi

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Work with each respective group owner to remediate this issue and ensure that the group ownership of their files are set to an appropriate value.

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

1.166 SOL-11.1-070130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Reserved UIDs 0-99 must only be used by system accounts.

```
GROUP ID: V-216192
RULE ID: SV-216192r959010
```

Rationale:

If a user is assigned a UID that is in the reserved range, even if it is not presently in use, security exposures can arise if a subsequently installed application uses the same UID.

Audit:

The root role is required.

Check that reserved UIDs are not assigned to non-system users.

Determine the OS version you are currently securing:

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

```
logins -so | awk -F: '{ print $1 }' | while read user; do
found=0
for tUser in root daemon bin sys adm dladm netadm netcfg
ftp dhcpserv sshd smmsp gdm zfssnap aiuser
polkitd ikeuser lp openldap webservd unknown
uucp nuucp upnp xvm mysql postgres svctag
pkg5srv nobody noaccess nobody4; do
if [ ${user} = ${tUser} ]; then
found=1
fi
done
if [ $found -eq 0 ]; then
echo "Invalid User with Reserved UID: ${user}"
fi
done
```

If output is produced without justification and documentation in accordance with site policy, this is a finding.

For Solaris 11.4 or newer:

```
logins -so | awk -F: '{ print $1 }' | while read user; do
found=0
for tUser in root daemon bin sys adm dladm netadm
netcfg dhcpserv sshd smmsp gdm zfssnap aiuser _polkitd
ikeuser lp openldap webservd unknown
```

uucp nuucp upnp xvm mysql postgres svctag

pkg5srv nobody noaccess nobody4 _ntp; do

if [${user} = ${tUser}]; then

found=1

fi

done

if [$found -eq 0]; then

echo "Invalid User with Reserved UID: ${user}"

fi

done

If output is produced without justification and documentation in accordance with site policy, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the Check step. Determine if there are any accounts using these reserved UIDs, and work with their owners to determine the best course of action in accordance with site policy. This may require deleting users or changing UIDs for users.

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

1.167 SOL-11.1-070140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Duplicate user names must not exist.

```
GROUP ID: V-216193
RULE ID: SV-216193r959010
```

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in passwd.

Audit:

The root role is required.

Identify any duplicate user names.

getent passwd | awk -F: '{print $1}' | uniq -d

If output is produced, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the Check step. Determine if there are any duplicate user names, and work with their respective owners to determine the best course of action in accordance with site policy. Delete or change the user name of duplicate users.

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

1.168 SOL-11.1-070150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Duplicate group names must not exist.

```
GROUP ID: V-216194
RULE ID: SV-216194r959010
```

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in group. Effectively, the GID is shared, which is a security risk.

Audit:

The root role is required.

Check for duplicate group names.

getent group | cut -f1 -d":" | sort -n | uniq -d

If output is produced, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the Check step. Determine if there are any duplicate group names, and work with their respective owners to determine the best course of action in accordance with site policy. Delete or change the group name of duplicate groups.

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

1.169 SOL-11.1-070160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

User .netrc files must not exist.

```
GROUP ID: V-216195
RULE ID: SV-216195r959010
```

Rationale:

The .netrc file presents a significant security risk since it stores passwords in unencrypted form.

Audit:

The root role is required.

Check for the presence of user .netrc files.

for dir in

logins -ox | awk -F: '($8 == "PS") { print $6 }'; do

ls -l ${dir}/.netrc 2>/dev/null

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Determine if any .netrc files exist, and work with the owners to determine the best course of action in accordance with site policy.

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

1.170 SOL-11.1-070170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must not allow users to configure .forward files.

```
GROUP ID: V-216196
RULE ID: SV-216196r959010
```

Rationale:

Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a secondary risk as it can be used to execute commands that may perform unintended actions.

Audit:

The root role is required.

for dir in

logins -ox | awk -F: '($8 == "PS") { print $6 }'; do

ls -l ${dir}/.forward 2>/dev/null

done

If output is produced, this is a finding.

Remediation:

The root role is required.

Remove any .forward files that are found.

pfexec rm [filename]

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

1.171 SOL-11.1-070180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

World-writable files must not exist.

```
GROUP ID: V-216197
RULE ID: SV-216197r959010
```

Rationale:

Data in world-writable files can be read, modified, and potentially compromised by any user on the system. World-writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

The root role is required.

Check for the existence of world-writable files.

find / (-fstype nfs -o -fstype cachefs -o -fstype autofs

-o -fstype ctfs -o -fstype mntfs -o -fstype objfs

-o -fstype proc) -prune -o -type f -perm -0002 -print

If output is produced, this is a finding.

Remediation:

The root role is required.

Change the permissions of the files identified in the check step to remove the world-writable permission.

pfexec chmod o-w [filename]

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

1.172 SOL-11.1-070190 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

All valid SUID/SGID files must be documented.

```
GROUP ID: V-216198
RULE ID: SV-216198r959010
```

Rationale:

There are valid reasons for SUID/SGID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

The root role is required.

find / (-fstype nfs -o -fstype cachefs -o -fstype autofs

-o -fstype ctfs -o -fstype mntfs -o -fstype objfs

-o -fstype proc) -prune -o -type f -perm -4000 -o

-perm -2000 -print

Output should only be Solaris-provided files and approved customer files.

Solaris-provided SUID/SGID files can be listed using the command:

pkg contents -a mode=4??? -a mode=2??? -t file -o pkg.name,path,mode

Digital signatures on the Solaris Set-UID binaries can be verified with the elfsign utility, such as this example:

elfsign verify -e /usr/bin/su

elfsign: verification of /usr/bin/su passed.

This message indicates that the binary is properly signed.

If non-vendor provided or non-approved files are included in the list, this is a finding.

Remediation:

The root role is required.

Determine the existence of any set-UID programs that do not belong on the system, and work with the owners (or system administrator) to determine the best course of action in accordance with site policy.

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

1.173 SOL-11.1-070200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must have no unowned files.

```
GROUP ID: V-216199
RULE ID: SV-216199r959010
```

Rationale:

A new user who is assigned a deleted user's user ID or group ID may then end up owning these files, and thus have more access on the system than was intended.

Audit:

The root role is required.

Identify all files that are owned by a user or group not listed in /etc/passwd or /etc/group

find / (-fstype nfs -o -fstype cachefs -o -fstype autofs

-o -fstype ctfs -o -fstype mntfs -o -fstype objfs

-o -fstype proc) -prune (-nouser -o -nogroup) -ls

If output is produced, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the Check step. Determine the existence of any files that are not attributed to current users or groups on the system, and determine the best course of action in accordance with site policy. Remove the files and directories or change their ownership.

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

1.174 SOL-11.1-070210 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must have no files with extended attributes.

```
GROUP ID: V-216200
RULE ID: SV-216200r959010
```

Rationale:

Attackers or malicious users could hide information, exploits, etc. in extended attribute areas. Since extended attributes are rarely used, it is important to find files with extended attributes set and correct these attributes.

Audit:

The root role is required.

Identify all files with extended attributes.

find / (-fstype nfs -o -fstype cachefs -o -fstype autofs

-o -fstype ctfs -o -fstype mntfs -o -fstype objfs

-o -fstype proc) -prune -o -xattr -ls

If output is produced, this is a finding.

Remediation:

The root role is required.

Correct or justify any items discovered in the Check step. Determine the existence of any files having extended file attributes, and determine the best course of action in accordance with site policy.

Remove the files or the extended attributes.

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

1.175 SOL-11.1-070220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The root account must be the only account with GID of 0.

```
GROUP ID: V-216201
RULE ID: SV-216201r959010
```

Rationale:

All accounts with a GID of 0 have root group privileges and must be limited to the group account only.

Audit:

Identify any users with GID of 0.

awk -F: '$4 == 0' /etc/passwd

awk -F: '$3 == 0' /etc/group

Confirm the only account with a group id of 0 is root.

If the root account is not the only account with GID of 0, this is a finding.

Remediation:

The root role is required.

Change the default GID of non-root accounts to a valid GID other than 0.

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

1.176 SOL-11.1-070240 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The operating system must reveal error messages only to authorized personnel.

```
GROUP ID: V-216202
RULE ID: SV-216202r958566
```

Rationale:

Proper file permissions and ownership ensures that only designated personnel in the organization can access error messages.

Audit:

Check the permissions of the /var/adm/messages file:

ls -l /var/adm/messages

Check the permissions of the /var/adm directory:

ls -ld /var/adm

If the owner and group of /var/adm/messages is not root and the permissions are not 640, this is a finding.

If the owner of /var/adm is not root, group is not sys, and the permissions are not 750, this is a finding.

Remediation:

The root role is required.

Change the permissions and owner on the /var/adm/messages file:

chmod 640 /var/adm/messages

chown root /var/adm/messages

chgrp root /var/adm/messages

Change the permissions and owner on the /var/adm directory:

chmod 750 /var/adm

chown root /var/adm

chgrp sys /var/adm

Additional Information:

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

1.177 SOL-11.1-070250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must protect the audit records resulting from non-local accesses to privileged accounts and the execution of privileged functions.

```
GROUP ID: V-220013
RULE ID: SV-220013r958732
```

Rationale:

Protection of audit records and audit data is of critical importance. Care must be taken to ensure privileged users cannot circumvent audit protections put in place. Auditing might not be reliable when performed by an operating system which the user being audited has privileged access to. The privileged user could inhibit auditing or directly modify audit records. To prevent this from occurring, privileged access shall be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

Audit:

The audit configuration profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the location of the local audit trail files.

auditconfig -getplugin audit_binfile

Plugin: audit_binfile (active)

Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=1;"

In this example, the audit files can be found in /var/audit. Check that the permissions on the audit files are 640 (rw- r-- --) or less permissive.

ls -al /var/audit

ls -l /var/audit/*

If the permissions are more permissive than 640, this is a finding.

Note: The default Solaris 11 location for /var/audit is a link to /var/share/audit.

Remediation:

The root role is required.

Determine the location of the local audit trail files.

pfexec auditconfig -getplugin audit_binfile

Plugin: audit_binfile (active)

Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=1

In this example, the audit files can be found in /var/audit.

Change the permissions on the audit trail files and the audit directory.

chmod 640 /var/share/audit/*

chmod 750 /var/share/audit

Note: The default Solaris 11 location for /var/audit is a link to /var/share/audit.

Additional Information:

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)
- NIST SP 800-53 Revision 5::AC-6 (9)

1.178 SOL-11.1-070260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operator must document all file system objects that have non-standard access control list settings.

```
GROUP ID: V-216204
RULE ID: SV-216204r959010
```

Rationale:

Access Control Lists allow an object owner to expand permissions on an object to specific users and groups in addition to the standard permission model. Non-standard Access Control List settings can allow unauthorized users to modify critical files.

Audit:

The root role is required.

Identify all file system objects that have non-standard access control lists enabled.

find / (-fstype nfs -o -fstype cachefs -o -fstype autofs

-o -fstype ctfs -o -fstype mntfs -o -fstype objfs

-o -fstype proc) -prune -o -acl -ls

This command should return no output. If output is created, this is a finding.

If the files are approved to have ACLs by organizational security policy, document the files and the reason that ACLs are required.

Remediation:

The root role is required.

Remove ACLs that are not approved in the security policy.

For ZFS file systems, remove all extended ACLs with the following command:

chmod A- [filename]

For UFS file systems

Determine the ACLs that are set on a file:

getfacl [filename]

Remove any ACL configurations that are set:

setfacl -d [ACL] [filename]

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

1.179 SOL-11.1-080010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must be a supported release.

```
GROUP ID: V-216205
RULE ID: SV-216205r959010
```

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:

Determine the operating system version.

uname -a

If the release is not supported by the vendor, this is a finding.

Remediation:

Upgrade to a supported version of the operating system.

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

1.180 SOL-11.1-080020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must implement non-executable program stacks.

```
GROUP ID: V-216206
RULE ID: SV-216206r959010
```

Rationale:

A common type of exploit is the stack buffer overflow. An application receives, from an attacker, more data than it is prepared for and stores this information on its stack, writing beyond the space reserved for it. This can be designed to cause execution of the data written on the stack. One mechanism to mitigate this vulnerability is for the system to not allow the execution of instructions in sections of memory identified as part of the stack.

Audit:

Determine the OS version you are currently securing.

uname –v

If the OS version is 11.3 or newer, this check applies to all zones and relies on the "sxadm" command. Determine if the system implements non-executable program stacks.

sxadm status -p nxstack | cut -d: -f2

enabled.all

If the command output is not "enabled.all", this is a finding.

For Solaris 11, 11.1, and 11.2, this check applies to the global zone only and the "/etc/system" file is inspected. Determine the zone that you are currently securing.

zonename

If the command output is "global", determine if the system implements non-executable program stacks.

grep noexec_user_stack /etc/system

If the noexec_user_stack is not set to 1, this is a finding.

Remediation:

The root role is required.

Determine the OS version you are currently securing.

uname –v

If the OS version is 11.3 or newer, enable non-executable program stacks using the "sxadm" command.

pfexec sxadm enable nxstack

For Solaris 11, 11.1, and 11.2, this action applies to the global zone only and the "/etc/system" file is updated. Determine the zone that you are currently securing.

zonename

If the command output is "global", modify the "/etc/system" file.

pfedit /etc/system

add the line:

set noexec_user_stack=1

Solaris 11, 11.1, and 11.2 systems will need to be restarted for the setting to take effect.

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

1.181 SOL-11.1-080030 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Address Space Layout Randomization (ASLR) must be enabled.

```
GROUP ID: V-216207
RULE ID: SV-216207r959010
```

Rationale:

Modification of memory area can result in executable code vulnerabilities. ASLR can reduce the likelihood of these attacks. ASLR activates the randomization of key areas of the process such as stack, brk-based heap, memory mappings, and so forth.

Audit:

This check applies to the global zone only.

Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine if address space layout randomization is enabled.

Determine the OS version you are currently securing:.

uname –v

For Solaris 11, 11.1, 11.2, and 11.3:

sxadm info -p | grep aslr | grep enabled

For Solaris 11.4 or newer:

sxadm status -p -o status aslr | grep enabled

If no output is produced, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Enable address space layout randomization.

sxadm delcust aslr

Enabling ASLR may affect the function or stability of some applications, including those that use Solaris Intimate Shared Memory features.

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

1.182 SOL-11.1-080040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Process core dumps must be disabled unless needed.

```
GROUP ID: V-216208
RULE ID: SV-216208r959010
```

Rationale:

Process core dumps contain the memory in use by the process when it crashed. Process core dump files can be of significant size and their use can result in file systems filling to capacity, which may result in denial of service. Process core dumps can be useful for software debugging.

Audit:

Check the process core dump configuration.

coreadm | grep enabled

If any lines are returned by coreadm other than "logging", this is a finding.

Remediation:

The Maintenance and Repair profile is required.

Change the process core dump configuration to disable core dumps globally and on a per process basis.

coreadm -d global

coreadm -d process

coreadm -d global-setid

coreadm -d proc-setid

coreadm -e log

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

1.183 SOL-11.1-080045 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The system must be configured to store any process core dumps in a specific, centralized directory.

```
GROUP ID: V-216209
RULE ID: SV-216209r959010
```

Rationale:

Specifying a centralized location for core file creation allows for the centralized protection of core files. Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If process core dump creation is not configured to use a centralized directory, core dumps may be created in a directory that does not have appropriate ownership or permissions configured, which could result in unauthorized access to the core dumps.

Audit:

Check the defined directory for process core dumps:

coreadm | grep "global core file pattern"

If the parameter is not set, or is not an absolute path (does not start with a slash [/]), this is a finding.

Remediation:

The root role is required.

Set the core file directory and file pattern.

coreadm -g /var/share/cores/core.%f.%p

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

1.184 SOL-11.1-080050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The centralized process core dump data directory must be owned by root.

```
GROUP ID: V-216210
RULE ID: SV-216210r959010
```

Rationale:

Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the centralized process core dump data directory is not owned by root, the core dumps contained in the directory may be subject to unauthorized access.

Audit:

Check the defined directory for process core dumps.

coreadm | grep "global core file pattern"

Check the ownership of the directory.

ls -lLd [core file directory]

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

Remediation:

The root role is required.

Change the owner of the core file directory.

chown root [core file directory]

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

1.185 SOL-11.1-080060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The centralized process core dump data directory must be group-owned by root, bin, or sys.

```
GROUP ID: V-216211
RULE ID: SV-216211r959010
```

Rationale:

Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the centralized process core dump data directory is not group-owned by a system group, the core dumps contained in the directory may be subject to unauthorized access.

Audit:

Check the defined directory for process core dumps.

coreadm | grep "global core file pattern"

Check the group ownership of the directory.

ls -lLd [core file directory]

If the directory is not group-owned by root, bin, or sys, this is a finding.

Remediation:

The root role is required.

Change the group-owner of the core file directory to root, bin or sys.

Example: chgrp root [core file directory]

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

1.186 SOL-11.1-080070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The centralized process core dump data directory must have mode 0700 or less permissive.

```
GROUP ID: V-216212
RULE ID: SV-216212r959010
```

Rationale:

Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the process core dump data directory has a mode more permissive than 0700, unauthorized users may be able to view or to modify sensitive information contained in any process core dumps in the directory.

Audit:

Check the defined directory for process core dumps.

coreadm | grep "global core file pattern"

Check the permissions of the directory.

ls -lLd [core file directory]

If the directory has a mode more permissive than 0700 (rwx --- ---), this is a finding.

Remediation:

The root role is required.

Change the mode of the core file directory.

chmod 0700 [core file directory]

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

1.187 SOL-11.1-080080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Kernel core dumps must be disabled unless needed.

```
GROUP ID: V-216213
RULE ID: SV-216213r959010
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system. The kernel core dump process may increase the amount of time a system is unavailable due to a crash. Kernel core dumps can be useful for kernel debugging.

Audit:

The root role is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Verify savecore is not used.

dumpadm | grep 'Savecore enabled'

If the value is yes, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Disable savecore.

dumpadm -n

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

1.188 SOL-11.1-080090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The kernel core dump data directory must be owned by root.

```
GROUP ID: V-216214
RULE ID: SV-216214r959010
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If the kernel core dump data directory is not owned by root, the core dumps contained in the directory may be subject to unauthorized access.

Audit:

The root role is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the location of the system dump directory.

dumpadm | grep directory

Check the ownership of the kernel core dump data directory.

ls -ld [savecore directory]

If the kernel core dump data directory is not owned by root, this is a finding.

In Solaris 11, /var/crash is linked to /var/share/crash.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Determine the location of the system dump directory.

dumpadm | grep directory

Change the owner of the kernel core dump data directory to root.

chown root [savecore directory]

In Solaris 11, /var/crash is linked to /var/share/crash.

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

1.189 SOL-11.1-080100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The kernel core dump data directory must be group-owned by root.

```
GROUP ID: V-216215
RULE ID: SV-216215r959010
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If the kernel core dump data directory is not group-owned by a system group, the core dumps contained in the directory may be subject to unauthorized access.

Audit:

The root role is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the location of the system dump directory.

dumpadm | grep directory

Check ownership of the core dump data directory.

ls -l [savecore directory]

If the directory is not group-owned by root, this is a finding.

In Solaris 11, /var/crash is linked to /var/share/crash.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Determine the location of the system dump directory.

dumpadm | grep directory

Change the group-owner of the kernel core dump data directory.

chgrp root [kernel core dump data directory]

In Solaris 11, /var/crash is linked to /var/share/crash.

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

1.190 SOL-11.1-080110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The kernel core dump data directory must have mode 0700 or less permissive.

```
GROUP ID: V-216216
RULE ID: SV-216216r959010
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If the mode of the kernel core dump data directory is more permissive than 0700, unauthorized users may be able to view or to modify kernel core dump data files.

Audit:

The root role is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Determine the location of the system dump directory.

dumpadm | grep directory

Check the permissions of the kernel core dump data directory.

ls -ld [savecore directory]

If the directory has a mode more permissive than 0700 (rwx --- ---), this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Determine the location of the system dump directory.

dumpadm | grep directory

Change the group-owner of the kernel core dump data directory.

chmod 0700 [savecore directory]

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

1.191 SOL-11.1-080120 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

System BIOS or system controllers supporting password protection must have administrator accounts/passwords configured, and no others. (Intel)

```
GROUP ID: V-216217
RULE ID: SV-216217r959010
```

Rationale:

A system's BIOS or system controller handles the initial startup of a system and its configuration must be protected from unauthorized modification. When the BIOS or system controller supports the creation of user accounts or passwords, such protections must be used and accounts/passwords only assigned to system administrators. Failure to protect BIOS or system controller settings could result in denial of service or compromise of the system resulting from unauthorized configuration changes.

Audit:

This check applies to X86 compatible platforms.

On systems with a BIOS or system controller, verify a supervisor or administrator password is set. If a password is not set, this is a finding.

If the BIOS or system controller supports user-level access in addition to supervisor/administrator access, determine if this access is enabled. If so, this is a finding.

Remediation:

Consult the hardware vendor's documentation to determine how to start the system and access the BIOS controls.

Access the system's BIOS or system controller. Set a supervisor/administrator password if one has not been set. Disable a user-level password if one has been set.

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

1.192 SOL-11.1-080140 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must require authentication before allowing modification of the boot devices or menus. Secure the GRUB Menu (Intel).

```
GROUP ID: V-216218
RULE ID: SV-216218r959010
```

Rationale:

The flexibility that GRUB provides creates a security risk if its configuration is modified by an unauthorized user. The failsafe menu entry needs to be secured in the same environments that require securing the systems firmware to avoid unauthorized removable media boots.

Audit:

This check applies to X86 systems only.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

grep source /rpool/boot/grub/grub.cfg

source $prefix/custom.cfg

If the output does not contain "source $prefix/custom.cfg" on a line of its own, this is a finding.

grep superusers /rpool/boot/grub/custom.cfg.

grep password_pbkdf2 /rpool/boot/grub/custom.cfg

If no superuser name and password are defined, this is a finding.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Update GRUB to use a custom configuration file.

pfedit /rpool/boot/grub/grub.cfg

Insert the line:

source $prefix/custom.cfg

Create a password hash.

/usr/lib/grub2/bios/bin/grub-mkpasswd-pbkdf2

Enter password:

Reenter password:

Your PBKDF2 is .....

Copy the long password hash in its entirety.

pfedit /rpool/boot/grub/custom.cfg

Insert the lines:

set superusers="[username]"

password_pbkdf2 [username] [password hash]

Restart the system.

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

1.193 SOL-11.1-080150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must implement transaction recovery for transaction-based systems.

```
GROUP ID: V-216219
RULE ID: SV-216219r959010
```

Rationale:

Recovery and reconstitution constitutes executing an operating system contingency plan comprised of activities to restore essential missions and business functions.

Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

While this is typically a database function, operating systems could be transactional in nature with respect to file processing.

Audit:

Solaris 11 ZFS copy-on-write model allows filesystem accesses to work according to a transactional model, such that on-disk content is always consistent and cannot be configured to be out of compliance.

Determine if any UFS file systems are mounted with the "nologging" option.

mount|grep nologging

If any file systems are listed, this is a finding.

Remediation:

The root role is required.

Solaris 11 ZFS copy-on-write model allows filesystem accesses to work according to a transactional model, such that on-disk content is always consistent and cannot be configured to be out of compliance.

If any UFS file systems are mounted with the "nologging" options, remove that option from the /etc/vfstab file.

pfedit /etc/vfstab

Locate any file systems listed with the "nologging" option and delete the keyword "nologging".

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

CCI-000553 Implement transaction recovery for systems that are transaction-based.

- NIST SP 800-53::CP-10 (2)
- NIST SP 800-53A::CP-10 (2).1
- NIST SP 800-53 Revision 4::CP-10 (2)
- NIST SP 800-53 Revision 5::CP-10 (2)

1.194 SOL-11.1-080160 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

SNMP communities, users, and passphrases must be changed from the default.

```
GROUP ID: V-216220
RULE ID: SV-216220r959010
```

Rationale:

Whether active or not, default SNMP passwords, users, and passphrases must be changed to maintain security. If the service is running with the default authenticators, then anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s).

Audit:

The root role is required.

Check the SNMP configuration for default passwords.

Locate and examine the SNMP configuration.

Procedure:

Find any occurrences of the snmpd.conf file delivered with Solaris packages:

pkg search -l -Ho path snmpd.conf | awk '{ print "/"$1 }'

more [filename]

Identify any community names or user password configurations. If any community name or password is set to a default value, such as public, private, snmp-trap, or password, this is a finding.

Remediation:

The root role is required.

Change the default snmpd.conf community passwords. To change them, locate the snmpd.conf file and edit it.

pfedit [filename]

Locate the line system-group-read-community which has a default password of public and make the password something more random (less guessable). Make the same changes for the lines that read system- group-write-community, read-community, write-community, trap, and trap-community. Read the information in the file carefully. The trap is defining who to send traps to, for instance, by default. It is not a password, but the name of a host.

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

1.195 SOL-11.1-090010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A file integrity baseline must be created, maintained, and reviewed at least weekly to determine if unauthorized changes have been made to important system files located in the root file system.

```
GROUP ID: V-216221
RULE ID: SV-216221r959010
```

Rationale:

A file integrity baseline is a collection of file metadata used to evaluate the integrity of the system. A minimal baseline must contain metadata for all device files, setuid files, setgid files, system libraries, system binaries, and system configuration files. The minimal metadata must consist of the mode, owner, group owner, and modification times. For regular files, metadata must also include file size and a cryptographic hash of the file's contents.

Audit:

The root role is required.

Solaris 11 includes the Basic Account and Reporting Tool (BART), which uses cryptographic-strength checksums and file system metadata to determine changes. By default, the manifest generator catalogs all attributes of all files in the root (/) file system. File systems mounted on the root file system are cataloged only if they are of the same type as the root file system.

A Baseline BART manifest may exist in:

/var/adm/log/bartlogs/[control manifest filename]

If a BART manifest does not exist, this is a finding.

At least weekly, create a new BART baseline report.

bart create > /var/adm/log/bartlogs/[new manifest filename]

Compare the new report to the previous report to identify any changes in the system baseline.

bart compare /var/adm/log/bartlogs/[baseline manifest filename] /var/adm/log/bartlogs/[new manifest filename]

Examine the BART report for changes. If there are changes to system files in /etc that are not approved, this is a finding.

Remediation:

The root role is required.

Solaris 11 includes the Basic Account and Reporting Tool (BART), which uses cryptographic-strength checksums and file system metadata to determine changes. By default, the manifest generator catalogs all attributes of all files in the root (/) file system. File systems mounted on the root file system are cataloged only if they are of the same type as the root file system.

Create a protected area to store BART manifests.

mkdir /var/adm/log/bartlogs

chmod 700 /var/adm/log/bartlogs

After initial installation and configuration of the system, create a manifest report of the current baseline.

bart create > /var/adm/log/bartlogs/[baseline manifest filename]

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

1.196 SOL-11.1-090020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must synchronize internal information system clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

```
GROUP ID: V-220014
RULE ID: SV-220014r1016297
```

Rationale:

To assure the accuracy of the system clock, it must be synchronized with an authoritative time source within DOD. Many system functions, including time-based login and activity restrictions, automated reports, system logs, and audit records depend on an accurate system clock. If there is no confidence in the correctness of the system clock, time-based functions may not operate as intended and records may be of diminished value.

Audit:

NTP must be used and used only in the global zone. Determine the zone to be secured.

zonename

If the command output is not "global", then NTP must be disabled. Check the system for a running NTP daemon.

svcs -Ho state ntp

If NTP is online, this is a finding.

If the output from "zonename" is "global", then NTP must be enabled. Check the system for a running NTP daemon.

svcs -Ho state ntp

If NTP is not online, this is a finding.

If NTP is running, confirm the servers and peers or multicast client (as applicable) are local or an authoritative U.S. DOD source.

For the NTP daemon:

more /etc/inet/ntp.conf

If a nonlocal/nonauthoritative (non-DOD source, non-USNO-based, or non-GPS) time server is used, this is a finding.

Determine if the time synchronization frequency is correct.

grep "maxpoll" /etc/inet/ntp.conf

If the command returns "File not found" or any value for maxpoll, this is a finding.

Determine if the running NTP server is configured properly.

ntpq -p | awk '($6 ~ /[0-9]+/ && $6 > 86400) { print $1" "$6 }'

This will print out the name of any time server whose current polling time is greater than 24 hours (along with the actual value). If there is any output, this is a finding.

Remediation:

The root role is required.

Determine the zone to be secured.

zonename

If the command output is not "global", then NTP must be disabled.

svcadm disable ntp

If the output from "zonename" is "global", then NTP must be enabled.

To activate the ntpd daemon, the ntp.conf file must first be created.

cp /etc/inet/ntp.client /etc/inet/ntp.conf

pfedit /etc/inet/ntp.conf

Make site-specific changes to this file as needed in the form.

server [ntpserver]

Locate the line containing maxpoll (if it exists).

Delete the line.

Start the ntpd daemon.

svcadm enable ntp

Use a local authoritative time server synchronizing to an authorized DOD time source, a USNO-based time server, or a GPS. Ensure all systems in the facility feed from one or more local time servers that feed from the authoritative time server.

Edit the NTP configuration files and make the necessary changes to add the approved time servers per Solaris documentation.

Additional Information:

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-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

1.197 SOL-11.1-090030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Direct logins must not be permitted to shared, default, application, or utility accounts.

```
GROUP ID: V-216223
RULE ID: SV-216223r959010
```

Rationale:

Shared accounts (accounts where two or more people log in with the same user identification) do not provide identification and authentication. There is no way to provide for non-repudiation or individual accountability.

Audit:

The Audit Review profile is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Use the "auditreduce" command to check for multiple accesses to an account

auditreduce -c lo -u [shared_user_name] | praudit -l

If users log directly into accounts, rather than using the "su" command from their own named account to access them, this is a finding. Also, ask the SA or the IAO if shared accounts are logged into directly or if users log into an individual account and switch user to the shared account.

Remediation:

The root role is required.

This action applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this action applies.

Use the switch user ("su") command from a named account login to access shared accounts. Maintain audit trails that identify the actual user of the account name. Document requirements and procedures for users/administrators to log into their own accounts first and then switch user ("su") to the shared account.

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

1.198 SOL-11.1-090040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The system must not have any unnecessary accounts.

```
GROUP ID: V-216224
RULE ID: SV-216224r959010
```

Rationale:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Audit:

Check the system for unnecessary user accounts.

getent passwd

Some examples of unnecessary accounts include games, news, gopher, ftp, and lp. If any unnecessary accounts are found, this is a finding.

Remediation:

The root role is required.

Remove all unnecessary accounts, such as games, from the /etc/passwd file before connecting a system to the network. Other accounts, such as news and gopher, associated with a service not in use should also be removed.

Identify unnecessary accounts.

getent passwd

Remove unnecessary accounts.

userdel [username]

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

1.199 SOL-11.1-090050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must conduct backups of user-level information contained in the operating system per organization-defined frequency to conduct backups consistent with recovery time and recovery point objectives.

```
GROUP ID: V-216225
RULE ID: SV-216225r959010
```

Rationale:

Operating system backup is a critical step in maintaining data assurance and availability.

User-level information is data generated by information system and/or application users.

Backups shall be consistent with organizational recovery time and recovery point objectives.

Audit:

The operations staff shall ensure that proper backups are created, tested, and archived.

Ask the operator for documentation on the backup procedures implemented.

If the backup procedures are not documented then this is a finding.

Remediation:

The operations staff shall install, configure, test, and verify operating system backup software.

Additionally, all backup procedures must be documented.

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

1.200 SOL-11.1-090060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must conduct backups of system-level information contained in the information system per organization-defined frequency to conduct backups that are consistent with recovery time and recovery point objectives.

```
GROUP ID: V-216226
RULE ID: SV-216226r959010
```

Rationale:

Operating system backup is a critical step in maintaining data assurance and availability.

System-level information is data generated for/by the host (such as configuration settings) and/or administrative users.

Backups shall be consistent with organizational recovery time and recovery point objectives.

Audit:

The operations staff shall ensure that proper backups are created, tested, and archived.

Ask the operator for documentation on the backup procedures implemented.

If the backup procedures are not documented then this is a finding.

Remediation:

The operations staff shall install, configure, test, and verify operating system backup software.

Additionally, all backup procedures must be documented.

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

1.201 SOL-11.1-090070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must conduct backups of operating system documentation including security-related documentation per organization-defined frequency to conduct backups that is consistent with recovery time and recovery point objectives.

```
GROUP ID: V-216227
RULE ID: SV-216227r959010
```

Rationale:

Operating system backup is a critical step in maintaining data assurance and availability.

System documentation is data generated for/by the host (such as logs) and/or administrative users.

Backups shall be consistent with organizational recovery time and recovery point objectives.

Audit:

The operations staff shall ensure that proper backups are created, tested, and archived.

Ask the operator for documentation on the backup procedures implemented.

If the backup procedures are not documented then this is a finding.

Remediation:

The operations staff shall install, configure, test, and verify operating system backup software.

Additionally, all backup procedures must be documented.

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

1.202 SOL-11.1-090100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent the execution of prohibited mobile code.

```
GROUP ID: V-216228
RULE ID: SV-216228r958544
```

Rationale:

Decisions regarding the employment of mobile code within operating systems are based on the potential for the code to cause damage to the system if used maliciously.

Mobile code technologies include Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

Audit:

Determine if the Firefox package is installed:

pkg list web/browser/firefox

If the package is not installed, this check does not apply.

If installed, ensure that it is a supported version.

pkg info firefox | grep Version

Version: 52.5.2

If the version is not supported, this is a finding.

Ensure that Java and JavaScript access by Firefox are disabled.

Start Firefox.

In the address bar type: about:config

In search bar type: javascript.enabled

If 'Value" is true, this is a finding

In the address bar type: about:addons

Click on "I accept the risk" button.

Click on "Plugins".

If Java is enabled, this is a finding.

Remediation:

In the address bar type: about:config

Click on "I accept the risk" button.

In search bar type: javascript.enabled

Double click on the javascript.enabled and Value true will change to false.

In the address bar type: about:addons

Click on "Plugins".

If Java is displayed, disable Java by clicking on the

Never Activate selection

Additional Information:

CCI-001695 Prevent the execution of organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (3)
- NIST SP 800-53 Revision 4::SC-18 (3)
- NIST SP 800-53 Revision 5::SC-18 (3)
- NIST SP 800-53A::SC-18 (3).1

1.203 SOL-11.1-090115 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ PKI solutions at workstations, servers, or mobile computing devices on the network to create, manage, distribute, use, store, and revoke digital certificates.

```
GROUP ID: V-216229
RULE ID: SV-216229r959010
```

Rationale:

Without the use of PKI systems to manage digital certificates, the operating system or other system components may be unable to securely communicate on a network or reliably verify the identity of a user via digital signatures.

Audit:

The operator will ensure that a DoD approved PKI system is installed, configured, and properly operating. Ask the operator to document the PKI software installation and configuration.

If the operator is not able to provide a documented configuration for an installed PKI system or if the PKI system is not properly configured, maintained, or used, this is a finding.

Remediation:

The operator will ensure that a DoD approved PKI software is installed and operating continuously.

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

1.204 SOL-11.1-090120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must prevent non-privileged users from circumventing malicious code protection capabilities.

```
GROUP ID: V-224672
RULE ID: SV-224672r958726
```

Rationale:

In order to minimize potential negative impact to the organization caused by malicious code, it is imperative that malicious code is identified and eradicated prior to entering protected enclaves via operating system entry and exit points.

The requirement states that AV and malware protection applications must be used at entry and exit points. For the operating system, this means an anti-virus application must be installed on machines that are the entry and exit points.

Audit:

The operator will ensure that anti-virus software is installed and operating.

If the operator is unable to provide a documented configuration for an installed anti-virus software system or if not properly used, this is a finding.

Remediation:

The operator will ensure that anti-virus software is installed and operating.

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)

1.205 SOL-11.1-090130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must employ malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means.

```
GROUP ID: V-216231
RULE ID: SV-216231r959010
```

Rationale:

In order to minimize potential negative impact to the organization caused by malicious code, it is imperative that malicious code is identified and eradicated prior to entering protected enclaves via operating system entry and exit points.

The requirement states that AV and malware protection applications must be used at entry and exit points. For the operating system, this means an anti-virus application must be installed on machines that are the entry and exit points.

Audit:

The operator will ensure that anti-virus software is installed and operating.

If the operator is unable to provide a documented configuration for an installed anti-virus software system or if not properly used, this is a finding.

Remediation:

The operator will ensure that anti-virus software is installed and operating.

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

1.206 SOL-11.1-090220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must back up audit records at least every seven days onto a different system or system component than the system or component being audited.

```
GROUP ID: V-216233
RULE ID: SV-216233r958574
```

Rationale:

Protection of log data includes assuring log data is not accidentally lost or deleted. Backing up audit records to a different system or onto separate media than the system being audited on an organizationally defined frequency helps to assure in the event of a catastrophic system failure, the audit records will be retained.

This helps to ensure a compromise of the information system being audited does not also result in a compromise of the audit records.

This requirement can be met by the operating system continuously sending records to a centralized logging server.

Audit:

This check applies to the global zone only. Determine the zone that you a currently securing.

zonename

If the command output is "global" this check applies.

The operator must back up audit records at least every 7 days.

If the operator is unable to provide a documented procedure or the documented procedure is not being followed, then this is a finding.

Remediation:

This fix applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The operator shall back up audit records at least every seven days.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.207 SOL-11.1-090240 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

All manual editing of system-relevant files shall be done using the pfedit command, which logs changes made to the files.

```
GROUP ID: V-216234
RULE ID: SV-216234r959010
```

Rationale:

Editing a system file with common tools such as vi, emacs, or gedit does not allow the auditing of changes made by an operator. This reduces the capability of determining which operator made security-relevant changes to the system.

Audit:

Ask the operators if they use vi, emacs, or gedit to make changes to system files.

If vi, emacs, or gedit are used to make changes to system files, this is a finding.

Remediation:

Advise the operators to use pdfedit or other appropriate command line tools to make system changes instead of vi, emacs, or gedit.

Oracle Solaris includes administrative configuration files which use pfedit, and the solaris.admin.edit/path_to_file authorization is not recommended. Alternate commands exist which are both domain-specific and safer. For example, for the /etc/passwd, /etc/shadow, or /etc/user_attr files, use instead passwd, useradd, userdel, or usermod. For the /etc/group file, use instead groupadd, groupdel, or groupmod. For updating /etc/security/auth_attr, /etc/security/exec_attr, or /etc/security/prof_attr, the preferred command is profiles.

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

1.208 SOL-11.1-090250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must verify the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification).

```
GROUP ID: V-220015
RULE ID: SV-220015r958944
```

Rationale:

Security functional testing involves testing the operating system for conformance to the operating system security function specifications, as well as for the underlying security model. The need to verify security functionality applies to all security functions. The conformance criteria state the conditions necessary for the operating system to exhibit the desired security behavior or satisfy a security property. For example, successful login triggers an audit entry.

Audit:

Ask the operator if DoD-approved SCAP compliance checking software is installed and run on a periodic basis.

If DoD-approved SCAP compliance checking software is not installed and/or not run on a periodic basis, this is a finding.

Remediation:

Install, configure, and run DoD-approved SCAP compliance checking software on a periodic basis. Review the output of the software and document any out-of-compliance issues.

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

1.209 SOL-11.1-090270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must identify potentially security-relevant error conditions.

```
GROUP ID: V-224673
RULE ID: SV-224673r958944
```

Rationale:

Security functional testing involves testing the operating system for conformance to the operating system security function specifications, as well as for the underlying security model. The need to verify security functionality applies to all security functions. The conformance criteria state the conditions necessary for the operating system to exhibit the desired security behavior or satisfy a security property. For example, successful login triggers an audit entry.

Audit:

Ask the operator if DoD-approved SCAP compliance checking software is installed and run on a periodic basis.

If DoD-approved SCAP compliance checking software is not installed and/or not run on a periodic basis, this is a finding.

Remediation:

Install, configure, and run DoD-approved SCAP compliance checking software on a periodic basis. Review the output of the software and document any out-of-compliance issues.

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

1.210 SOL-11.1-090280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

```
GROUP ID: V-216237
RULE ID: SV-216237r958528
```

Rationale:

In the case of denial of service attacks, care must be taken when designing the operating system so as to ensure that the operating system makes the best use of system resources.

Audit:

Verify that you are on the global zone:

zoneadm -z global list

global

Note: If you see following message, you are not in the global zone:

```
"zoneadm: global: No such zone exists"
```

dladm show-ether -Z | egrep "LINK|up"

LINK PTYPE STATE AUTO SPEED-DUPLEX PAUSE

net0 current up yes 1G-f bi

Determine the OS version that is being secured:

uname -v

For Solaris 11, 11.1, 11.2, and 11.3:

dladm show-linkprop net0 | egrep "LINK|en_" | sort|uniq

LINK PROPERTY PERM VALUE EFFECTIVE DEFAULT POSSIBLE

net0 en_1000fdx_cap rw 1 1 1 1,0

net0 en_1000hdx_cap r- 0 0 0 1,0

net0 en_100fdx_cap rw 1 1 1 1,0

net0 en_100hdx_cap rw 1 1 1 1,0

net0 en_10fdx_cap rw 1 1 1 1,0

net0 en_10gfdx_cap -- -- -- 0 1,0

net0 en_10hdx_cap rw 1 1 1 1,0

Do the above for all available/connected network adapters.

For Solaris 11.4.x.x.x or newer:

dladm show-linkprop -p speed-duplex net0

LINK PROPERTY PERM VALUE EFFECTIVE DEFAULT POSSIBLE

net0 speed-duplex rw 1g-f,100m-f, 1g-f,100m-f, 1g-f, 1g-f,100m-f,

100m-h, 100m-h, 100m-f, 100m-h,10m-f,

10m-f,10m-h 10m-f,10m-h 100m-h, 10m-h

10m-f,

10m-h

Do the above for all available/connected network adapters.

For each link, determine if its current speed-duplex settings VALUE field is appropriate for managing any excess bandwidth capacity based on its POSSIBLE settings field; if not, this is a finding.

Remediation:

The Network Management profile is required.

Set each link's speed-duplex protection to an appropriate value based on each configured network interface's POSSIBLE settings.

Determine the OS version that is being secured:

uname -a

For Solaris 11, 11.1, 11.2, and 11.3:

pfexec dladm set-linkprop -p en_1000fdx_cap=1 net0

Verify EFFECTIVE column

dladm show-linkprop net0 | egrep "LINK|en_" | sort|uniq

LINK PROPERTY PERM VALUE EFFECTIVE DEFAULT POSSIBLE

net0 en_1000fdx_cap rw 1 1 1 1,0

net0 en_1000hdx_cap r- 0 0 0 1,0

net0 en_100fdx_cap rw 1 1 1 1,0

net0 en_100hdx_cap rw 1 1 1 1,0

net0 en_10fdx_cap rw 1 1 1 1,0

net0 en_10gfdx_cap -- -- -- 0 1,0

net0 en_10hdx_cap rw 1 1 1 1,0

Do the above for all available/connected network adapters.

For Solaris 11.4.x or newer:

pfexec dladm set-linkprop -p speed-duplex=1g-f,100m-f net0

Verify EFFECTIVE column

dladm show-linkprop -p speed-duplex net0

LINK PROPERTY PERM VALUE EFFECTIVE DEFAULT POSSIBLE

net0 speed-duplex rw 1g-f,100m-f 1g-f,100m-f 1g-f, 1g-f,100m-f,

100m-f, 100m-h,10m-f,

100m-h, 10m-h

10m-f,

10m-h

Do the above for all available/connected network adapters.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

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

1.211 SOL-11.1-100010 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The /etc/zones directory, and its contents, must have the vendor default owner, group, and permissions.

```
GROUP ID: V-216238
RULE ID: SV-216238r959010
```

Rationale:

Incorrect ownership can result in unauthorized changes or theft of data.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

Check the ownership of the files and directories.

pkg verify system/zones

The command should return no output. If output is produced, this is a finding.

Remediation:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The Software Installation profile is required.

Change the ownership and permissions of the files and directories to the factory default.

pkg fix system/zones

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

1.212 SOL-11.1-100020 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The limitpriv zone option must be set to the vendor default or less permissive.

```
GROUP ID: V-216239
RULE ID: SV-216239r959010
```

Rationale:

Solaris zones can be assigned privileges generally reserved for the global zone using the "limitpriv" zone option. Any privilege assignments in excess of the vendor defaults may provide the ability for a non-global zone to compromise the global zone.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

List the non-global zones on the system.

zoneadm list -vi | grep -v global

From the output list of non-global zones found, determine if any are Kernel zones.

zoneadm list -cv | grep [zonename] | grep solaris-kz

Exclude any Kernel zones found from the list of local zones.

List the configuration for each zone.

zonecfg -z [zonename] info |grep limitpriv

If the output of this command has a setting for limitpriv and it is not:

limitpriv: default

this is a finding.

Remediation:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The Zone Security profile is required:

Change the "limitpriv" setting to default.

pfexec zonecfg -z [zone] set limitpriv=default

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

1.213 SOL-11.1-100030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The systems physical devices must not be assigned to non-global zones.

```
GROUP ID: V-216240
RULE ID: SV-216240r959010
```

Rationale:

Solaris non-global zones can be assigned physical hardware devices. This increases the risk of such a non-global zone having the capability to compromise the global zone.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

List the non-global zones on the system.

zoneadm list -vi | grep -v global

List the configuration for each zone.

zonecfg -z [zonename] info | grep dev

Check for device lines. If such a line exists and is not approved by security, this is a finding.

Remediation:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

The Zone Security profile is required:

Remove all device assignments from the non-global zone.

pfexec zonecfg -z [zone] delete device [device]

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

1.214 SOL-11.1-100040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The audit system must identify in which zone an event occurred.

```
GROUP ID: V-216241
RULE ID: SV-216241r959010
```

Rationale:

Tracking the specific Solaris zones in the audit trail reduces the time required to determine the cause of a security event.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

List the non-global zones on the system.

zoneadm list -vi | grep -v global

The Audit Configuration profile is required.

Determine whether the "zonename" auditing policy is in effect.

pfexec auditconfig -getpolicy | grep active | grep zonename

If no output is returned, this is a finding.

Remediation:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

List the non-global zones on the system.

zoneadm list -vi | grep -v global

The Audit Configuration profile is required.

Enable the "zonename" auditing policy.

pfexec auditconfig -setpolicy +zonename

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

1.215 SOL-11.1-100050 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The audit system must maintain a central audit trail for all zones.

```
GROUP ID: V-216242
RULE ID: SV-216242r959010
```

Rationale:

Centralized auditing simplifies the investigative process to determine the cause of a security event.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

List the non-global zones on the system.

zoneadm list -vi | grep -v global

The Audit Configuration profile is required.

Determine whether the "perzone" auditing policy is in effect.

pfexec auditconfig -getpolicy | grep active | grep perzone

If output is returned, this is a finding.

Remediation:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global", this check applies.

List the non-global zones on the system.

zoneadm list -vi | grep -v global

The Audit Configuration profile is required.

Disable the "perzone" auditing policy.

pfexec auditconfig -setpolicy -perzone

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

1.216 SOL-11.1-120410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must monitor for unauthorized connections of mobile devices to organizational information systems.

```
GROUP ID: V-216243
RULE ID: SV-216243r959010
```

Rationale:

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, audio recording devices).

Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements.

Usage restrictions and implementation guidance related to mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared).

In order to detect unauthorized mobile device connections, organizations must first identify and document what mobile devices are authorized.

Audit:

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global" this check applies.

Determine if USB mass storage devices are locked out by the kernel.

grep -h "exclude: scsa2usb" /etc/system /etc/system.d/*

If the output of this command is not:

exclude: scsa2usb

this is a finding.

Remediation:

The root role is required.

This check applies to the global zone only. Determine the zone that you are currently securing.

zonename

If the command output is "global" this check applies.

Modify the /etc/system file.

Determine the OS version you are currently securing.

uname –v

For Solaris 11GA and 11.1

pfedit /etc/system

Add a line containing:

exclude: scsa2usb

Note that the global zone will need to be rebooted for this change to take effect.

For Solaris 11.2 or newer

Modify an /etc/system.d file.

pfedit /etc/system.d/USB:MassStorage

Add a line containing:

exclude: scsa2usb

Note that the global zone will need to be rebooted for this change to take effect.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	SOL-11.1-010040 (Manual)	☐	☐
1.2	SOL-11.1-010060 (Manual)	☐	☐
1.3	SOL-11.1-010070 (Manual)	☐	☐
1.4	SOL-11.1-010080 (Manual)	☐	☐
1.5	SOL-11.1-010100 (Manual)	☐	☐
1.6	SOL-11.1-010120 (Manual)	☐	☐
1.7	SOL-11.1-010130 (Manual)	☐	☐
1.8	SOL-11.1-010140 (Manual)	☐	☐
1.9	SOL-11.1-010150 (Manual)	☐	☐
1.10	SOL-11.1-010160 (Manual)	☐	☐
1.11	SOL-11.1-010170 (Manual)	☐	☐
1.12	SOL-11.1-010180 (Manual)	☐	☐
1.13	SOL-11.1-010220 (Manual)	☐	☐
1.14	SOL-11.1-010230 (Manual)	☐	☐
1.15	SOL-11.1-010250 (Manual)	☐	☐
1.16	SOL-11.1-010260 (Manual)	☐	☐
1.17	SOL-11.1-010270 (Manual)	☐	☐
1.18	SOL-11.1-010290 (Manual)	☐	☐
1.19	SOL-11.1-010300 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	SOL-11.1-010310 (Manual)	☐	☐
1.21	SOL-11.1-010320 (Manual)	☐	☐
1.22	SOL-11.1-010330 (Manual)	☐	☐
1.23	SOL-11.1-010340 (Manual)	☐	☐
1.24	SOL-11.1-010350 (Manual)	☐	☐
1.25	SOL-11.1-010360 (Manual)	☐	☐
1.26	SOL-11.1-010370 (Manual)	☐	☐
1.27	SOL-11.1-010380 (Manual)	☐	☐
1.28	SOL-11.1-010390 (Manual)	☐	☐
1.29	SOL-11.1-010400 (Manual)	☐	☐
1.30	SOL-11.1-010410 (Manual)	☐	☐
1.31	SOL-11.1-010420 (Manual)	☐	☐
1.32	SOL-11.1-010440 (Manual)	☐	☐
1.33	SOL-11.1-020010 (Manual)	☐	☐
1.34	SOL-11.1-020020 (Manual)	☐	☐
1.35	SOL-11.1-020030 (Manual)	☐	☐
1.36	SOL-11.1-020040 (Manual)	☐	☐
1.37	SOL-11.1-020050 (Manual)	☐	☐
1.38	SOL-11.1-020080 (Manual)	☐	☐
1.39	SOL-11.1-020090 (Manual)	☐	☐
1.40	SOL-11.1-020100 (Manual)	☐	☐
1.41	SOL-11.1-020110 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	SOL-11.1-020120 (Manual)	☐	☐
1.43	SOL-11.1-020130 (Manual)	☐	☐
1.44	SOL-11.1-020140 (Manual)	☐	☐
1.45	SOL-11.1-020150 (Manual)	☐	☐
1.46	SOL-11.1-020160 (Manual)	☐	☐
1.47	SOL-11.1-020170 (Manual)	☐	☐
1.48	SOL-11.1-020180 (Manual)	☐	☐
1.49	SOL-11.1-020190 (Manual)	☐	☐
1.50	SOL-11.1-020220 (Manual)	☐	☐
1.51	SOL-11.1-020230 (Manual)	☐	☐
1.52	SOL-11.1-020300 (Manual)	☐	☐
1.53	SOL-11.1-020310 (Manual)	☐	☐
1.54	SOL-11.1-020320 (Manual)	☐	☐
1.55	SOL-11.1-020330 (Manual)	☐	☐
1.56	SOL-11.1-020340 (Manual)	☐	☐
1.57	SOL-11.1-020350 (Manual)	☐	☐
1.58	SOL-11.1-020360 (Manual)	☐	☐
1.59	SOL-11.1-020370 (Manual)	☐	☐
1.60	SOL-11.1-020380 (Manual)	☐	☐
1.61	SOL-11.1-020500 (Manual)	☐	☐
1.62	SOL-11.1-020510 (Manual)	☐	☐
1.63	SOL-11.1-020520 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	SOL-11.1-020530 (Manual)	☐	☐
1.65	SOL-11.1-020540 (Manual)	☐	☐
1.66	SOL-11.1-020550 (Manual)	☐	☐
1.67	SOL-11.1-020560 (Manual)	☐	☐
1.68	SOL-11.1-030010 (Manual)	☐	☐
1.69	SOL-11.1-030030 (Manual)	☐	☐
1.70	SOL-11.1-030040 (Manual)	☐	☐
1.71	SOL-11.1-030050 (Manual)	☐	☐
1.72	SOL-11.1-030060 (Manual)	☐	☐
1.73	SOL-11.1-040010 (Manual)	☐	☐
1.74	SOL-11.1-040020 (Manual)	☐	☐
1.75	SOL-11.1-040030 (Manual)	☐	☐
1.76	SOL-11.1-040040 (Manual)	☐	☐
1.77	SOL-11.1-040060 (Manual)	☐	☐
1.78	SOL-11.1-040070 (Manual)	☐	☐
1.79	SOL-11.1-040080 (Manual)	☐	☐
1.80	SOL-11.1-040090 (Manual)	☐	☐
1.81	SOL-11.1-040100 (Manual)	☐	☐
1.82	SOL-11.1-040110 (Manual)	☐	☐
1.83	SOL-11.1-040120 (Manual)	☐	☐
1.84	SOL-11.1-040130 (Manual)	☐	☐
1.85	SOL-11.1-040140 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	SOL-11.1-040160 (Manual)	☐	☐
1.87	SOL-11.1-040170 (Manual)	☐	☐
1.88	SOL-11.1-040180 (Manual)	☐	☐
1.89	SOL-11.1-040190 (Manual)	☐	☐
1.90	SOL-11.1-040200 (Manual)	☐	☐
1.91	SOL-11.1-040230 (Manual)	☐	☐
1.92	SOL-11.1-040250 (Manual)	☐	☐
1.93	SOL-11.1-040260 (Manual)	☐	☐
1.94	SOL-11.1-040270 (Manual)	☐	☐
1.95	SOL-11.1-040280 (Manual)	☐	☐
1.96	SOL-11.1-040310 (Manual)	☐	☐
1.97	SOL-11.1-040320 (Manual)	☐	☐
1.98	SOL-11.1-040330 (Manual)	☐	☐
1.99	SOL-11.1-040331 (Manual)	☐	☐
1.100	SOL-11.1-040340 (Manual)	☐	☐
1.101	SOL-11.1-040350 (Manual)	☐	☐
1.102	SOL-11.1-040360 (Manual)	☐	☐
1.103	SOL-11.1-040370 (Manual)	☐	☐
1.104	SOL-11.1-040380 (Manual)	☐	☐
1.105	SOL-11.1-040390 (Manual)	☐	☐
1.106	SOL-11.1-040400 (Manual)	☐	☐
1.107	SOL-11.1-040410 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	SOL-11.1-040420 (Manual)	☐	☐
1.109	SOL-11.1-040430 (Manual)	☐	☐
1.110	SOL-11.1-040450 (Manual)	☐	☐
1.111	SOL-11.1-040460 (Manual)	☐	☐
1.112	SOL-11.1-040470 (Manual)	☐	☐
1.113	SOL-11.1-040480 (Manual)	☐	☐
1.114	SOL-11.1-040490 (Manual)	☐	☐
1.115	SOL-11.1-040500 (Manual)	☐	☐
1.116	SOL-11.1-050010 (Manual)	☐	☐
1.117	SOL-11.1-050020 (Manual)	☐	☐
1.118	SOL-11.1-050030 (Manual)	☐	☐
1.119	SOL-11.1-050040 (Manual)	☐	☐
1.120	SOL-11.1-050050 (Manual)	☐	☐
1.121	SOL-11.1-050060 (Manual)	☐	☐
1.122	SOL-11.1-050070 (Manual)	☐	☐
1.123	SOL-11.1-050080 (Manual)	☐	☐
1.124	SOL-11.1-050090 (Manual)	☐	☐
1.125	SOL-11.1-050100 (Manual)	☐	☐
1.126	SOL-11.1-050110 (Manual)	☐	☐
1.127	SOL-11.1-050120 (Manual)	☐	☐
1.128	SOL-11.1-050130 (Manual)	☐	☐
1.129	SOL-11.1-050140 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	SOL-11.1-050240 (Manual)	☐	☐
1.131	SOL-11.1-050370 (Manual)	☐	☐
1.132	SOL-11.1-050380 (Manual)	☐	☐
1.133	SOL-11.1-050390 (Manual)	☐	☐
1.134	SOL-11.1-050410 (Manual)	☐	☐
1.135	SOL-11.1-050430 (Manual)	☐	☐
1.136	SOL-11.1-050460 (Manual)	☐	☐
1.137	SOL-11.1-050470 (Manual)	☐	☐
1.138	SOL-11.1-050480 (Manual)	☐	☐
1.139	SOL-11.1-060010 (Manual)	☐	☐
1.140	SOL-11.1-060060 (Manual)	☐	☐
1.141	SOL-11.1-060070 (Manual)	☐	☐
1.142	SOL-11.1-060080 (Manual)	☐	☐
1.143	SOL-11.1-060090 (Manual)	☐	☐
1.144	SOL-11.1-060100 (Manual)	☐	☐
1.145	SOL-11.1-060110 (Manual)	☐	☐
1.146	SOL-11.1-060120 (Manual)	☐	☐
1.147	SOL-11.1-060130 (Manual)	☐	☐
1.148	SOL-11.1-060140 (Manual)	☐	☐
1.149	SOL-11.1-060150 (Manual)	☐	☐
1.150	SOL-11.1-060160 (Manual)	☐	☐
1.151	SOL-11.1-060170 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	SOL-11.1-060180 (Manual)	☐	☐
1.153	SOL-11.1-060190 (Manual)	☐	☐
1.154	SOL-11.1-070010 (Manual)	☐	☐
1.155	SOL-11.1-070020 (Manual)	☐	☐
1.156	SOL-11.1-070030 (Manual)	☐	☐
1.157	SOL-11.1-070040 (Manual)	☐	☐
1.158	SOL-11.1-070050 (Manual)	☐	☐
1.159	SOL-11.1-070060 (Manual)	☐	☐
1.160	SOL-11.1-070070 (Manual)	☐	☐
1.161	SOL-11.1-070080 (Manual)	☐	☐
1.162	SOL-11.1-070090 (Manual)	☐	☐
1.163	SOL-11.1-070100 (Manual)	☐	☐
1.164	SOL-11.1-070110 (Manual)	☐	☐
1.165	SOL-11.1-070120 (Manual)	☐	☐
1.166	SOL-11.1-070130 (Manual)	☐	☐
1.167	SOL-11.1-070140 (Manual)	☐	☐
1.168	SOL-11.1-070150 (Manual)	☐	☐
1.169	SOL-11.1-070160 (Manual)	☐	☐
1.170	SOL-11.1-070170 (Manual)	☐	☐
1.171	SOL-11.1-070180 (Manual)	☐	☐
1.172	SOL-11.1-070190 (Manual)	☐	☐
1.173	SOL-11.1-070200 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	SOL-11.1-070210 (Manual)	☐	☐
1.175	SOL-11.1-070220 (Manual)	☐	☐
1.176	SOL-11.1-070240 (Manual)	☐	☐
1.177	SOL-11.1-070250 (Manual)	☐	☐
1.178	SOL-11.1-070260 (Manual)	☐	☐
1.179	SOL-11.1-080010 (Manual)	☐	☐
1.180	SOL-11.1-080020 (Manual)	☐	☐
1.181	SOL-11.1-080030 (Manual)	☐	☐
1.182	SOL-11.1-080040 (Manual)	☐	☐
1.183	SOL-11.1-080045 (Manual)	☐	☐
1.184	SOL-11.1-080050 (Manual)	☐	☐
1.185	SOL-11.1-080060 (Manual)	☐	☐
1.186	SOL-11.1-080070 (Manual)	☐	☐
1.187	SOL-11.1-080080 (Manual)	☐	☐
1.188	SOL-11.1-080090 (Manual)	☐	☐
1.189	SOL-11.1-080100 (Manual)	☐	☐
1.190	SOL-11.1-080110 (Manual)	☐	☐
1.191	SOL-11.1-080120 (Manual)	☐	☐
1.192	SOL-11.1-080140 (Manual)	☐	☐
1.193	SOL-11.1-080150 (Manual)	☐	☐
1.194	SOL-11.1-080160 (Manual)	☐	☐
1.195	SOL-11.1-090010 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.196	SOL-11.1-090020 (Manual)	☐	☐
1.197	SOL-11.1-090030 (Manual)	☐	☐
1.198	SOL-11.1-090040 (Manual)	☐	☐
1.199	SOL-11.1-090050 (Manual)	☐	☐
1.200	SOL-11.1-090060 (Manual)	☐	☐
1.201	SOL-11.1-090070 (Manual)	☐	☐
1.202	SOL-11.1-090100 (Manual)	☐	☐
1.203	SOL-11.1-090115 (Manual)	☐	☐
1.204	SOL-11.1-090120 (Manual)	☐	☐
1.205	SOL-11.1-090130 (Manual)	☐	☐
1.206	SOL-11.1-090220 (Manual)	☐	☐
1.207	SOL-11.1-090240 (Manual)	☐	☐
1.208	SOL-11.1-090250 (Manual)	☐	☐
1.209	SOL-11.1-090270 (Manual)	☐	☐
1.210	SOL-11.1-090280 (Manual)	☐	☐
1.211	SOL-11.1-100010 (Manual)	☐	☐
1.212	SOL-11.1-100020 (Manual)	☐	☐
1.213	SOL-11.1-100030 (Manual)	☐	☐
1.214	SOL-11.1-100040 (Manual)	☐	☐
1.215	SOL-11.1-100050 (Manual)	☐	☐
1.216	SOL-11.1-120410 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08/29/2025	1.0.0	Initial CIS Release