CIS VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 STIG Benchmark

v1.0.0 – 08-01-2024

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

VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

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 VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 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 VMware vSphere 8.0 vCenter Appliance Photon OS 4.0

Recommendations

1 STIG RULES

VMware vSphere

VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

CLASSIFICATION unclassified

1.1 PHTN-40-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account creations.

```
GROUP ID: V-258801
RULE ID: SV-258801r958368
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000476-GPOS-00221

Audit:

At the command line, run the following command to verify an audit rule exists to audit account creations:

auditctl -l | grep -E "(useradd|groupadd)"

Example result:

-w /usr/sbin/useradd -p x -k useradd -w /usr/sbin/groupadd -p x -k groupadd

If either "useradd" or "groupadd" are not listed with a permissions filter of at least "x", this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-w /usr/sbin/useradd -p x -k useradd -w /usr/sbin/groupadd -p x -k groupadd

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

Additional Information:

CCI-000018 Automatically audit account creation actions.

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

CCI-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

1.2 PHTN-40-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period.

```
GROUP ID: V-258802
RULE ID: SV-258802r958388
```

Rationale:

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

Audit:

At the command line, run the following commands to verify accounts are locked after three consecutive invalid logon attempts by a user during a 15-minute time period:

grep '^deny =' /etc/security/faillock.conf

Example result:

deny = 3

If the "deny" option is not set to "3" or less (but not "0"), is missing or commented out, this is a finding.

grep '^fail_interval =' /etc/security/faillock.conf

Example result:

fail_interval = 900

If the "fail_interval" option is not set to "900" or more, is missing or commented out, this is a finding.

Note: If faillock.conf is not used to configure the "pam_faillock.so" module, then these options may be specified on the faillock lines in the system-auth and system-account PAM files.

Remediation:

Navigate to and open:

/etc/security/faillock.conf

Add or update the following lines:

deny = 3 fail_interval = 900

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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

1.3 PHTN-40-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Photon operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.

```
GROUP ID: V-258804
RULE ID: SV-258804r958398
```

Rationale:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to Denial of Service (DoS) attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

Audit:

At the command line, run the following command to verify the limit for the number of concurrent sessions:

grep "^[^].*maxlogins.*" /etc/security/limits.conf

Example result:

- `hard    maxlogins       10`
-

If "* hard maxlogins" is not configured to "10", this is a finding.

Note: The expected result may be repeated multiple times.

Remediation:

Navigate to and open:

/etc/security/limits.conf

Add or update the following line:

- `hard    maxlogins       10`
-

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

1.4 PHTN-40-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system.

```
GROUP ID: V-258803
RULE ID: SV-258803r958390
```

Rationale:

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

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

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"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."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

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

Audit:

At the command line, run the following command to verify SSH is configured to use the /etc/issue file for a banner:

sshd -T|&grep -i Banner

Example result:

banner /etc/issue

If the "banner" setting is not configured to "/etc/issue", this is a finding.

Next, open /etc/issue with a text editor.

If the file does not contain the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

Standard Mandatory DOD Notice and Consent Banner:

"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."

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "Banner" line is uncommented and set to the following:

Banner /etc/issue

Navigate to and open:

/etc/issue

Ensure the file contains the Standard Mandatory DOD Notice and Consent Banner.

"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."

At the command line, run the following command:

systemctl restart sshd.service

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

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

1.5 PHTN-40-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must monitor remote access logins.

```
GROUP ID: V-258805
RULE ID: SV-258805r958406
```

Rationale:

Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best. Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. Automated monitoring of remote access sessions allows organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

If another package is used to offload logs, such as syslog-ng, and is properly configured, this is not applicable.

At the command line, run the following command to verify rsyslog is configured to log authentication requests:

grep -E "(^auth.|^*authpriv.*|^daemon.*)" /etc/rsyslog.conf

Example result:

auth.*;authpriv.*;daemon.* /var/log/audit/sshinfo.log

If "auth.*", "authpriv.*", and "daemon.*" are not configured to be logged, this is a finding.

Remediation:

Navigate to and open:

/etc/rsyslog.conf

Add or update the following line:

auth.*;authpriv.*;daemon.* /var/log/audit/sshinfo.log

Note: The path can be substituted for another suitable log destination dedicated to authentication logs.

At the command line, run the following command:

systemctl restart rsyslog.service

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)

1.6 PHTN-40-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must have the OpenSSL FIPS provider installed to protect the confidentiality of remote access sessions.

```
GROUP ID: V-258806
RULE ID: SV-258806r958408
```

Rationale:

Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session.

OpenSSH on the Photon operating system when configured appropriately can utilize a FIPS validated OpenSSL for cryptographic operations.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000423-GPOS-00187, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

At the command line, run the following command to verify the OpenSSL FIPS provider is installed:

rpm -qa | grep openssl-fips

Example result:

openssl-fips-provider-3.0.3-1.ph4.x86_64

If there is no output indicating that the OpenSSL FIPS provider is installed, this is a finding.

Remediation:

At the command line, run the following command:

tdnf install openssl-fips-provider

Additional Information:

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

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

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

CCI-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

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)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

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

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

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

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

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

1.7 PHTN-40-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure auditd to log to disk.

```
GROUP ID: V-258807
RULE ID: SV-258807r958412
```

Rationale:

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content must be shipped to a central location, but it must also be logged locally.

Audit:

At the command line, run the following command to verify auditd is configured to write logs to disk:

grep '^write_logs' /etc/audit/auditd.conf

Example result:

write_logs = yes

If there is no output, this is not a finding.

If "write_logs" exists and is not configured to "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Ensure the "write_logs" line is uncommented and set to the following:

write_logs = yes

At the command line, run the following command:

pkill -SIGHUP auditd

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

1.8 PHTN-40-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enable the auditd service.

```
GROUP ID: V-258808
RULE ID: SV-258808r1003628
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. To that end, the auditd service must be configured to start automatically and be running at all times.

Satisfies: SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000062-GPOS-00031, SRG-OS-000255-GPOS-00096, SRG-OS-000363-GPOS-00150, SRG-OS-000365-GPOS-00152, SRG-OS-000446-GPOS-00200

Audit:

At the command line, run the following command to verify auditd is enabled and running:

systemctl status auditd

If the service is not enabled and running, this is a finding.

Remediation:

At the command line, run the following commands:

systemctl enable auditd systemctl start auditd

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

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

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

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

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

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

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

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

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-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)

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

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

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4::SI-6 b
- NIST SP 800-53 Revision 5::SI-6 b

1.9 PHTN-40-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must alert the ISSO and SA in the event of an audit processing failure.

```
GROUP ID: V-258810
RULE ID: SV-258810r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000344-GPOS-00135

Audit:

At the command line, run the following command to verify auditd is configured to send an alert via syslog in the event of an audit processing failure:

grep -E "^disk_full_action|^disk_error_action|^admin_space_left_action" /etc/audit/auditd.conf

Example result:

admin_space_left_action = SYSLOG disk_full_action = SYSLOG disk_error_action = SYSLOG

If "disk_full_action", "disk_error_action", and "admin_space_left_action" are not set to SYSLOG or are missing, this is a finding.

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Ensure the following lines are present, not duplicated, and not commented:

disk_full_action = SYSLOG disk_error_action = SYSLOG admin_space_left_action = SYSLOG

At the command line, run the following command:

pkill -SIGHUP auditd

Additional Information:

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

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

CCI-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)

1.10 PHTN-40-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to audit the execution of privileged functions.

```
GROUP ID: V-258809
RULE ID: SV-258809r958422
```

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing all actions by superusers is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000326-GPOS-00126

Audit:

At the command line, run the following command to verify audit rules exist to audit privileged functions:

auditctl -l | grep execve

Expected result:

-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F key=execpriv -a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F key=execpriv -a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -F key=execpriv -a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -F key=execpriv

If the output does not match the expected result, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F key=execpriv -a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F key=execpriv -a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -F key=execpriv -a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -F key=execpriv

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

Additional Information:

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

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

CCI-002233 Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4::AC-6 (8)
- NIST SP 800-53 Revision 5::AC-6 (8)

1.11 PHTN-40-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must protect audit logs from unauthorized access.

```
GROUP ID: V-258811
RULE ID: SV-258811r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

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

Audit:

At the command line, run the following command to find the current auditd log location:

grep -iw log_file /etc/audit/auditd.conf

Example result:

log_file = /var/log/audit/audit.log

At the command line, run the following command using the file found in the previous step to verify auditd logs are protected from authorized access:

stat -c "%n %U:%G %a" /var/log/audit/audit.log

Example result:

/var/log/audit/audit.log root:root 600

If the audit log file does not have permissions set to "0600", this is a finding. If the audit log file is not owned by root, this is a finding. If the audit log file is not group owned by root, this is a finding.

Remediation:

At the command line, run the following commands:

chmod 0600 chown root:root

Replace with the target log file.

Note: If "log_group" is configured in the auditd.conf file and set to something other than "root", the permissions changes will not be persistent.

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

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

CCI-000163 Protect audit information from unauthorized modification.

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

CCI-000164 Protect audit information from unauthorized deletion.

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

1.12 PHTN-40-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must allow only authorized users to configure the auditd service.

```
GROUP ID: V-258812
RULE ID: SV-258812r958444
```

Rationale:

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

At the command line, run the following command to verify permissions on auditd configuration and rules files:

find /etc/audit/* -type f -exec stat -c "%n %U:%G %a" {} $1;

If any files are returned with permissions more permissive than "0640", this is a finding. If any files are returned not owned by root, this is a finding. If any files are returned not group owned by root, this is a finding.

Remediation:

At the command line, run the following commands:

chmod 0640 chown root:root

Replace with the target file.

Additional Information:

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

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

1.13 PHTN-40-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must generate audit records when successful/unsuccessful attempts to access privileges occur.

```
GROUP ID: V-258813
RULE ID: SV-258813r958446
```

Rationale:

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000474-GPOS-00219

Audit:

At the command line, run the following command to verify an audit rule exists to audit account creations:

auditctl -l | grep chmod

Expected result:

-a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod -a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid=0 -F key=perm_mod -a always,exit -F arch=b32 -S chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod -a always,exit -F arch=b32 -S chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid=0 -F key=perm_mod

If the output does not match the expected result, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Note: auid!=-1, auid!=4294967295, auid!=unset are functionally equivalent in this check and the output of the above commands may be displayed in either format.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid=0 -F key=perm_mod -a always,exit -F arch=b32 -S chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b32 -S chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr,fchownat,fchmodat -F auid=0 -F key=perm_mod

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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

1.14 PHTN-40-000035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-258814
RULE ID: SV-258814r1003629
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

At the command line, run the following command to verify at least one uppercase character be used:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "ucredit" option is not < 0, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "ucredit" option set to "-1" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.15 PHTN-40-000036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-258815
RULE ID: SV-258815r1003630
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

At the command line, run the following command to verify at least one lowercase character be used:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "lcredit" option is not < 0, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "lcredit" option set to "-1" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.16 PHTN-40-000037 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-258816
RULE ID: SV-258816r1003631
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

At the command line, run the following command to verify at least one numeric character be used:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "dcredit" option is not < 0, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "dcredit" option set to "-1" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.17 PHTN-40-000038 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must require the change of at least eight characters when passwords are changed.

```
GROUP ID: V-258817
RULE ID: SV-258817r1003632
```

Rationale:

If the operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least eight characters.

Audit:

At the command line, run the following command to verify at least eight different characters be used:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "difok" option is not >= 8, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "difok" option set to "8" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.18 PHTN-40-000039 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The operating system must store only encrypted representations of passwords.

```
GROUP ID: V-258818
RULE ID: SV-258818r1003633
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

At the command line, run the following command to verify passwords are stored with only encrypted representations:

grep ^ENCRYPT_METHOD /etc/login.defs

Example result:

ENCRYPT_METHOD SHA512

If the "ENCRYPT_METHOD" option is not set to "SHA512", is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or update the following line:

ENCRYPT_METHOD SHA512

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)

1.19 PHTN-40-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must not have the telnet package installed.

```
GROUP ID: V-258819
RULE ID: SV-258819r987796
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

At the command line, run the following command to verify telnet is not installed:

rpm -qa | grep telnet

If any results are returned indicating telnet is installed, this is a finding.

Remediation:

At the command line, run the following command:

tdnf remove

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)

1.20 PHTN-40-000041 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce one day as the minimum password lifetime.

```
GROUP ID: V-258820
RULE ID: SV-258820r1003634
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

At the command line, run the following command to verify one day as the minimum password lifetime:

grep '^PASS_MIN_DAYS' /etc/login.defs

If "PASS_MIN_DAYS" is not set to 1, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or update the following line:

PASS_MIN_DAYS 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)

1.21 PHTN-40-000042 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating systems must enforce a 90-day maximum password lifetime restriction.

```
GROUP ID: V-258821
RULE ID: SV-258821r1003636
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

At the command line, run the following command to verify a 90-day maximum password lifetime restriction:

grep '^PASS_MAX_DAYS' /etc/login.defs

If "PASS_MAX_DAYS" is not set to <= 90, is missing or commented out, this is a finding. If "PASS_MAX_DAYS" is disabled or set to -1, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or update the following line:

PASS_MAX_DAYS 90

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)

1.22 PHTN-40-000043 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must prohibit password reuse for a minimum of five generations.

```
GROUP ID: V-258822
RULE ID: SV-258822r1003637
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

Audit:

At the command line, run the following commands to verify passwords are not reused for a minimum of five generations:

grep '^password.*pam_pwhistory.so' /etc/pam.d/system-password

Example result:

password required pam_pwhistory.so remember=5 retry=3 enforce_for_root use_authtok

If the "remember" option is not set to "5" or greater, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwhistory.so line to have the "remember" option set to 5 or greater as follows:

password required pam_pwhistory.so remember=5 retry=3 enforce_for_root use_authtok

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

Additional Information:

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

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

1.23 PHTN-40-000044 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce a minimum 15-character password length.

```
GROUP ID: V-258823
RULE ID: SV-258823r1003638
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

At the command line, run the following command to verify a minimum 15-character password length:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "minlen" option is not >= 15, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "minlen" option set to "15" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.24 PHTN-40-000046 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must require authentication upon booting into single-user and maintenance modes.

```
GROUP ID: V-258824
RULE ID: SV-258824r958472
```

Rationale:

If the system does not require authentication before it boots into single-user mode, anyone with console access to the system can trivially access all files on the system. GRUB2 is the boot loader for Photon OS and can be configured to require a password to boot into single-user mode or make modifications to the boot menu.

Note: Photon does not support building grub changes via grub2-mkconfig.

Audit:

At the command line, run the following command to verify a password is required to edit the grub bootloader to boot into single-user mode:

grep -E "^set\ssuperusers|^password_pbkdf2" /boot/grub2/grub.cfg

Example output:

set superusers="root" password_pbkdf2 root grub.pbkdf2.sha512.[password_hash]

If superusers is not set, this is a finding. If a password is not set for the super user, this is a finding.

Remediation:

Before proceeding, ensure a snapshot is taken to rollback if needed.

At the command line, run the following command to generate a grub password:

grub2-mkpasswd-pbkdf2

Enter a secure password and ensure this password is stored for break-glass situations. Users will not be able to recover the root account without knowing this separate password. Copy the resulting encrypted string.

An example string is below:

grub.pbkdf2.sha512.10000.983A13DF3C51BB2B5130F0B86DDBF0DEA1AAF766BD1F16B7840F79CE3E35494C4B99F505C99C150071E563DF1D7FE1F45456D5960C4C79DAB6C49298B02A5558.5B2C49E12D43CC5A876F6738462DE4EFC24939D4BE486CDB72CFBCD87FDE93FBAFCB817E01B90F23E53C2502C3230502BC3113BE4F80B0AFC0EE956E735F7F86

Note: The grub2 package must be installed to generate a password for grub.

Navigate to and open:

/boot/grub2/grub.cfg

Find the line that begins with "set rootpartition". Below this line, paste the following on its own line:

set superusers="root"

Note: The superusers name can be a value other than root and is not tied to an OS account.

Below this paste the following, substituting the user's own encrypted string from the steps above:

password_pbkdf2 root <YOUR-LONG-STRING-FROM-ABOVE>

Next edit the default Photon menuentry block with the "--unrestricted" parameter so that it will continue to boot without prompting for credentials, for example:

menuentry "Photon" --unrestricted { linux /boot/$photon_linux root=$rootpartition $photon_cmdline $systemd_cmdline audit=1 if [-f /boot/$photon_initrd]; then initrd /boot/$photon_initrd fi }

When booting now, if users press "e" when the Photon splash screen appears, users will be prompted for credentials before being presented the option to edit the boot loader before system startup.

Note: Photon does not support building grub changes via grub2-mkconfig.

Additional Information:

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

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

1.25 PHTN-40-000047 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must disable unnecessary kernel modules.

```
GROUP ID: V-258825
RULE ID: SV-258825r1003641
```

Rationale:

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

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

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

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000114-GPOS-00059

Audit:

At the command line, run the following command to verify the following kernel modules are not loaded:

modprobe --showconfig | grep "^install" | grep "/bin"

Expected result:

install sctp /bin/false install dccp /bin/false install dccp_ipv4 /bin/false install dccp_ipv6 /bin/false install ipx /bin/false install appletalk /bin/false install decnet /bin/false install rds /bin/false install tipc /bin/false install bluetooth /bin/false install usb_storage /bin/false install ieee1394 /bin/false install cramfs /bin/false install freevxfs /bin/false install jffs2 /bin/false install hfs /bin/false install hfsplus /bin/false install squashfs /bin/false install udf /bin/false

The output may include other statements outside of the expected result.

If the output does not include at least every statement in the expected result, this is a finding.

Remediation:

Navigate to and open:

/etc/modprobe.d/modprobe.conf

Set the contents as follows:

install sctp /bin/false install dccp /bin/false install dccp_ipv4 /bin/false install dccp_ipv6 /bin/false install ipx /bin/false install appletalk /bin/false install decnet /bin/false install rds /bin/false install tipc /bin/false install bluetooth /bin/false install usb_storage /bin/false install ieee1394 /bin/false install cramfs /bin/false install freevxfs /bin/false install jffs2 /bin/false install hfs /bin/false install hfsplus /bin/false install squashfs /bin/false install udf /bin/false

Additional Information:

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

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

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.26 PHTN-40-000049 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not have duplicate User IDs (UIDs).

```
GROUP ID: V-258826
RULE ID: SV-258826r958482
```

Rationale:

To ensure accountability and prevent unauthenticated access, organizational users must be uniquely identified and authenticated to prevent potential misuse and provide for nonrepudiation.

Audit:

At the command line, run the following command to verify there are no duplicate user IDs present:

awk -F ":" 'list[$3]++{print $1, $3}' /etc/passwd

If any lines are returned, this is a finding.

Remediation:

Navigate to and open:

/etc/passwd

Configure each user account that has a duplicate UID with a unique 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

1.27 PHTN-40-000059 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must use mechanisms meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

```
GROUP ID: V-258827
RULE ID: SV-258827r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DOD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2/140-3 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DOD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Audit:

At the command line, run the following command to verify system-password is configured to encrypt representations of passwords:

grep sha512 /etc/pam.d/system-password

Example result:

password required pam_unix.so sha512 shadow use_authtok

If the "pam_unix.so" module is not configured with the "sha512" parameter, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add or update the following line:

password required pam_unix.so sha512 shadow use_authtok

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

1.28 PHTN-40-000067 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must restrict access to the kernel message buffer.

```
GROUP ID: V-258828
RULE ID: SV-258828r958524
```

Rationale:

Restricting access to the kernel message buffer limits access only to root. This prevents attackers from gaining additional system information as a nonprivileged user.

Audit:

At the command line, run the following command to verify kernel message buffer restrictions are enabled:

/sbin/sysctl kernel.dmesg_restrict

Example result:

kernel.dmesg_restrict = 1

If the "kernel.dmesg_restrict" kernel parameter is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

kernel.dmesg_restrict = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1

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

1.29 PHTN-40-000068 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to use TCP syncookies.

```
GROUP ID: V-258829
RULE ID: SV-258829r958528
```

Rationale:

A TCP SYN flood attack can cause a Denial of Service (DOS) by filling a system's TCP connection table with connections in the SYN_RCVD state. Syncookies can be used to track a connection when a subsequent ACK is received, verifying the initiator is attempting a valid connection and is not a flood source. This feature is activated when a flood condition is detected and enables the system to continue servicing valid connection requests.

Satisfies: SRG-OS-000142-GPOS-00071, SRG-OS-000420-GPOS-00186

Audit:

At the command line, run the following command to verify TCP syncookies are enabled:

/sbin/sysctl net.ipv4.tcp_syncookies

Example result:

net.ipv4.tcp_syncookies = 1

If "net.ipv4.tcp_syncookies" is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

net.ipv4.tcp_syncookies = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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)

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

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

1.30 PHTN-40-000069 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must terminate idle Secure Shell (SSH) sessions after 15 minutes.

```
GROUP ID: V-258830
RULE ID: SV-258830r970703
```

Rationale:

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

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level, and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000395-GPOS-00175

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i ClientAliveInterval

Example result:

ClientAliveInterval 900

If there is no output or if "ClientAliveInterval" is not set to "900", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "ClientAliveInterval" line is uncommented and set to the following:

ClientAliveInterval 900

At the command line, run the following command:

systemctl restart sshd.service

Additional Information:

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

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

CCI-002891 Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

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

1.31 PHTN-40-000073 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system /var/log directory must be restricted.

```
GROUP ID: V-258831
RULE ID: SV-258831r958564
```

Rationale:

Any operating system providing too much information in error messages risks compromising the data and security of the structure, and content of error messages needs to be carefully considered by the organization.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, social security numbers, and credit card numbers.

Audit:

At the command line, run the following command to verify permissions on the /var/log directory:

stat -c "%n is owned by %U and group owned by %G with permissions of %a" /var/log

Expected result:

/var/log is owned by root and group owned by root with permissions of 755

If the /var/log directory is not owned by root, this is a finding. If the /var/log directory is not group owned by root, this is a finding. If the /var/log directory permissions are not set to 0755 or less, this is a finding.

Remediation:

At the command line, run the following commands:

chown root:root /var/log chmod 0755 /var/log

Additional Information:

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

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

1.32 PHTN-40-000074 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must reveal error messages only to authorized users.

```
GROUP ID: V-258832
RULE ID: SV-258832r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

Audit:

If another package is used to offload logs, such as syslog-ng, and is properly configured, this is not applicable.

At the command line, run the following command to verify rsyslog generates log files that are not world readable:

grep '^$umask' /etc/rsyslog.conf

Example result:

$umask 0037

If "$umask" is not set to "0037" or more restrictive, this is a finding.

Remediation:

Navigate to and open:

/etc/rsyslog.conf

Add or update the following line:

$umask 0037

At the command line, run the following command:

systemctl restart rsyslog.service

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

1.33 PHTN-40-000076 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account modifications.

```
GROUP ID: V-258833
RULE ID: SV-258833r991551
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to modify an existing account. Auditing account modification actions provides logging that can be used for forensic purposes.

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

Audit:

At the command line, run the following command to verify an audit rule exists to audit account modifications:

auditctl -l | grep -E "(usermod|groupmod)"

Example result:

-w /usr/sbin/usermod -p x -k usermod -w /usr/sbin/groupmod -p x -k groupmod

If either "usermod" or "groupmod" are not listed with a permissions filter of at least "x", this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-w /usr/sbin/usermod -p x -k usermod -w /usr/sbin/groupmod -p x -k groupmod

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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)

1.34 PHTN-40-000078 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account removal actions.

```
GROUP ID: V-258834
RULE ID: SV-258834r991553
```

Rationale:

When operating system accounts are removed, user accessibility is affected. Accounts are utilized for identifying individual users or for identifying the operating system processes themselves. In order to detect and respond to events affecting user accessibility and system processing, operating systems must audit account removal actions and, as required, notify the appropriate individuals so they can investigate the event. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and provides logging that can be used for forensic purposes.

Audit:

At the command line, run the following command to verify an audit rule exists to audit account removals:

auditctl -l | grep -E "(userdel|groupdel)"

Example result:

-w /usr/sbin/userdel -p x -k userdel -w /usr/sbin/groupdel -p x -k groupdel

If either "userdel" or "groupdel" are not listed with a permissions filter of at least "x", this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-w /usr/sbin/userdel -p x -k userdel -w /usr/sbin/groupdel -p x -k groupdel

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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)

1.35 PHTN-40-000079 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must implement only approved ciphers to protect the integrity of remote access sessions.

```
GROUP ID: V-258835
RULE ID: SV-258835r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i Ciphers

Expected result:

ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

If the output matches the ciphers in the expected result or a subset thereof, this is not a finding.

If the ciphers in the output contain any ciphers not listed in the expected result, this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "Ciphers" line is uncommented and set to the following:

Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

At the command line, run the following command:

systemctl restart sshd.service

Additional Information:

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)

1.36 PHTN-40-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must initiate session audits at system startup.

```
GROUP ID: V-258836
RULE ID: SV-258836r991555
```

Rationale:

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit:

At the command line, run the following command to verify auditing is enabled at startup:

grep 'audit' /proc/cmdline

Example result:

BOOT_IMAGE=/boot/vmlinuz-5.10.109-2.ph4-esx root=PARTUUID=6e6293c6-9ab6-49e9-aa97-9b212f2e037a init=/lib/systemd/systemd rcupdate.rcu_expedited=1 rw systemd.show_status=1 quiet noreplace-smp cpu_init_udelay=0 plymouth.enable=0 systemd.legacy_systemd_cgroup_controller=yes audit=1

If the "audit" parameter is not present with a value of "1", this is a finding.

Remediation:

Navigate to and open:

/boot/grub2/grub.cfg

Locate the boot command line arguments. An example follows:

linux /boot/$photon_linux root=$rootpartition $photon_cmdline $systemd_cmdline

Add "audit=1" to the end of the line so it reads as follows:

linux /boot/$photon_linux root=$rootpartition $photon_cmdline $systemd_cmdline audit=1

Note: Do not copy/paste in this example argument line. This may change in future releases. Find the similar line and append "audit=1" to it.

Reboot the system for the change to take effect.

Additional Information:

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

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

1.37 PHTN-40-000082 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must protect audit tools from unauthorized access.

```
GROUP ID: V-258837
RULE ID: SV-258837r991557
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

At the command line, run the following command to verify permissions on audit tools:

stat -c "%n is owned by %U and group owned by %G and permissions are %a" /usr/sbin/audispd /usr/sbin/auditctl /usr/sbin/auditd /usr/sbin/aureport /usr/sbin/ausearch /usr/sbin/autrace /usr/sbin/augenrules

Expected result:

/usr/sbin/audispd is owned by root and group owned by root and permissions are 750
/usr/sbin/auditctl is owned by root and group owned by root and permissions are 755
/usr/sbin/auditd is owned by root and group owned by root and permissions are 755
/usr/sbin/aureport is owned by root and group owned by root and permissions are 755
/usr/sbin/ausearch is owned by root and group owned by root and permissions are 755
/usr/sbin/autrace is owned by root and group owned by root and permissions are 755
/usr/sbin/augenrules is owned by root and group owned by root and permissions are 750

If any file is not owned by root or group owned by root or permissions are more permissive than listed above, this is a finding.

Remediation:

At the command line, run the following commands for each file returned:

chown root:root chmod 750

Note: Update permissions to match the target file as listed in the check text.

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

CCI-001494 Protect audit tools from unauthorized modification.

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

CCI-001495 Protect audit tools from unauthorized deletion.

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

1.38 PHTN-40-000086 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-258838
RULE ID: SV-258838r1003642
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity or strength is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ $ % ^ *.

Audit:

At the command line, run the following command to verify at least one special character be used:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "ocredit" option is not < 0, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "ocredit" option set to "-1" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.39 PHTN-40-000092 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must use cryptographic mechanisms to protect the integrity of audit tools.

```
GROUP ID: V-258839
RULE ID: SV-258839r991567
```

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Audit:

Use the verification capability of rpm to check the MD5 hashes of the audit files on disk versus the expected ones from the installation package.

At the command line, run the following command:

rpm -V audit | grep "^..5"

Example output:

S.5....T. c /etc/audit/auditd.conf

If there is any output for files that are not configuration files, this is a finding.

Remediation:

If the audit system binaries have been altered investigate the cause and then reinstall the audit package to restore the integrity of the package.

If performed on a VMware reinstalling the audit tools is not supported. The appliance should be restored from a backup or redeployed once the root cause is remediated.

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)

1.40 PHTN-40-000093 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The operating system must automatically terminate a user session after inactivity time-outs have expired.

```
GROUP ID: V-258840
RULE ID: SV-258840r1003643
```

Rationale:

Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific operating system functionality where the system owner, data owner, or organization requires additional assurance.

Satisfies: SRG-OS-000279-GPOS-00109, SRG-OS-000126-GPOS-00066

Audit:

At the command line, run the following command:

grep -E "TMOUT=900" /etc/bash.bashrc /etc/profile.d/*

Example result:

/etc/profile.d/tmout.sh:TMOUT=900

If the "TMOUT" environmental variable is not set, the value is more than "900", or is set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/profile.d/tmout.sh

Set its content to the following:

TMOUT=900 readonly TMOUT export TMOUT mesg n 2>/dev/null

Additional Information:

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

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

1.41 PHTN-40-000105 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must enable symlink access control protection in the kernel.

```
GROUP ID: V-258841
RULE ID: SV-258841r958726
```

Rationale:

By enabling the fs.protected_symlinks kernel parameter, symbolic links are permitted to be followed only when outside a sticky world-writable directory, or when the UID of the link and follower match, or when the directory owner matches the symlink's owner. Disallowing such symlinks helps mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Audit:

At the command line, run the following command to verify symlink protection is enabled:

/sbin/sysctl fs.protected_symlinks

Example result:

fs.protected_symlinks = 1

If the "fs.protected_symlinks" kernel parameter is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

fs.protected_symlinks = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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)

1.42 PHTN-40-000107 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit the execution of privileged functions.

```
GROUP ID: V-258842
RULE ID: SV-258842r1003645
```

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000240-GPOS-00090, SRG-OS-000458-GPOS-00203, SRG-OS-000463-GPOS-00207, SRG-OS-000471-GPOS-00215

Audit:

At the command line, run the following command to output a list of files with setuid/setgid configured and their corresponding audit rules:

for file in $(find / -xdev -path /var/lib/containerd -prune -o -path /var/lib/docker -prune -o (-perm -4000 -o -perm -2000) -type f -print | sort); do echo "Found file with setuid/setgid configured: $file";rule="$(auditctl -l | grep "$file ")";echo "Audit Rule Result: $rule";echo ""; done

Example output:

Found file with setuid/setgid configured: /usr/bin/chage Audit Rule Result: -a always,exit -S all -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged

Found file with setuid/setgid configured: /usr/bin/chfn Audit Rule Result: -a always,exit -S all -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged

If each file returned does not have a corresponding audit rule, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Note: auid!=-1, auid!=4294967295, auid!=unset are functionally equivalent in this check and the output of the above commands may be displayed in either format.

Remediation:

Run the following steps for each file found in the check that does not have a corresponding line in the audit rules:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add the following line:

-a always,exit -F path= -F perm=x -F auid>=1000 -F auid!=unset -F key=privileged

Run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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

CCI-001404 Automatically audit account disabling actions.

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

CCI-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)

1.43 PHTN-40-000108 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes occur.

```
GROUP ID: V-258843
RULE ID: SV-258843r958736
```

Rationale:

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

Audit:

At the command line, run the following commands to verify accounts are locked until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes are made:

grep '^unlock_time =' /etc/security/faillock.conf

Example result:

unlock_time = 0

If the "unlock_time" option is not set to "0", is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/security/faillock.conf

Add or update the following lines:

unlock_time = 0

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

Additional Information:

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

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

1.44 PHTN-40-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Photon operating system must allocate audit record storage capacity to store audit records when audit records are not immediately sent to a central audit record storage facility.

```
GROUP ID: V-258844
RULE ID: SV-258844r958752
```

Rationale:

Audit logs are most useful when accessible by date, rather than size. This can be accomplished through a combination of an audit log rotation and setting a reasonable number of logs to keep. This ensures that audit logs are accessible to the ISSO in the event of a central log processing failure.

Audit:

At the command line, run the following command to verify auditd is configured to keep a number of audit logs in the event of a central log processing failure:

grep -E "^num_logs|^max_log_file_action" /etc/audit/auditd.conf

Example result:

num_logs = 5 max_log_file_action = ROTATE

If "num_logs" is not configured to "5" or greater, this is a finding. If "max_log_file_action" is not configured to "ROTATE", this is a finding.

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Ensure the following lines are present, not duplicated, and not commented:

num_logs = 5 max_log_file_action = ROTATE

At the command line, run the following command:

pkill -SIGHUP auditd

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

1.45 PHTN-40-000112 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Photon operating system must immediately notify the SA and ISSO when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-258845
RULE ID: SV-258845r971542
```

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

At the command line, run the following command to verify auditd is alerting when low disk space is detected:

grep '^space_left' /etc/audit/auditd.conf

Expected result:

space_left = 25% space_left_action = SYSLOG

If the output does not match the expected result, this is a finding.

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Ensure the "space_left" and "space_left_action" lines are uncommented and set to the following:

space_left = 25% space_left_action = SYSLOG

At the command line, run the following command:

pkill -SIGHUP auditd

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)

1.46 PHTN-40-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system TDNF package management tool must cryptographically verify the authenticity of all software packages during installation.

```
GROUP ID: V-258846
RULE ID: SV-258846r1003646
```

Rationale:

Installation of any nontrusted software, patches, service packs, device drivers, or operating system components can significantly affect the overall security of the operating system. This requirement ensures the software has not been tampered with and has been provided by a trusted vendor.

Audit:

At the command line, run the following command to verify software packages are cryptographically verified during installation:

grep '^gpgcheck' /etc/tdnf/tdnf.conf

Example result:

gpgcheck=1

If "gpgcheck" is not set to "true", "1", or "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/tdnf/tdnf.conf

Add or update the following line:

gpgcheck=1

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

1.47 PHTN-40-000133 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must require users to reauthenticate for privilege escalation.

```
GROUP ID: V-258847
RULE ID: SV-258847r1003647
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

At the command line, run the following commands to verify users with a set password are not allowed to sudo without reauthentication:

grep -ihs nopasswd /etc/sudoers /etc/sudoers.d/*|grep -vE '(^|^%)'

awk -F: '($2 != "x" && $2 != "!") {print $1}' /etc/shadow

If any account listed in the first output is also listed in the second output and is not documented, this is a finding.

Remediation:

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

visudo

OR

visudo -f /etc/sudoers.d/

Remove any occurrences of "NOPASSWD" tags associated with user accounts with a password hash.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

1.48 PHTN-40-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must implement address space layout randomization to protect its memory from unauthorized code execution.

```
GROUP ID: V-258848
RULE ID: SV-258848r958928
```

Rationale:

Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

Audit:

At the command line, run the following command to verify address space layout randomization is enabled:

cat /proc/sys/kernel/randomize_va_space

If the value of "randomize_va_space" is not "2", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

kernel.randomize_va_space=2

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

Additional Information:

CCI-002824 Implement organization-defined controls to protect the system memory from unauthorized code execution.

- NIST SP 800-53 Revision 4::SI-16
- NIST SP 800-53 Revision 5::SI-16

1.49 PHTN-40-000161 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must remove all software components after updated versions have been installed.

```
GROUP ID: V-258849
RULE ID: SV-258849r958936
```

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

At the command line, run the following command:

grep -i '^clean_requirements_on_remove' /etc/tdnf/tdnf.conf

Example result:

clean_requirements_on_remove=1

If "clean_requirements_on_remove" is not set to "true", "1", or "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/tdnf/tdnf.conf

Add or update the following line:

clean_requirements_on_remove=1

Additional Information:

CCI-002617 Remove previous versions of organization-defined software components after updated versions have been installed.

- NIST SP 800-53 Revision 4::SI-2 (6)
- NIST SP 800-53 Revision 5::SI-2 (6)

1.50 PHTN-40-000173 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must generate audit records when successful/unsuccessful logon attempts occur.

```
GROUP ID: V-258850
RULE ID: SV-258850r991578
```

Rationale:

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

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

Audit:

At the command line, run the following command to verify an audit rule exists to audit logon attempts:

auditctl -l | grep -E "faillog|lastlog|tallylog"

Expected result:

-w /var/log/faillog -p wa -k logons -w /var/log/lastlog -p wa -k logons -w /var/log/tallylog -p wa -k logons

If the output does not match the expected result, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-w /var/log/faillog -p wa -k logons -w /var/log/lastlog -p wa -k logons -w /var/log/tallylog -p wa -k logons

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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

1.51 PHTN-40-000182 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

```
GROUP ID: V-258852
RULE ID: SV-258852r959006
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000478-GPOS-00223, SRG-OS-000396-GPOS-00176

Audit:

At the command line, run the following command to verify FIPS is enabled for the OS:

cat /proc/sys/crypto/fips_enabled

Example result:

1

If "fips_enabled" is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/boot/grub2/grub.cfg

Locate the boot command line arguments. An example follows:

linux /boot/$photon_linux root=$rootpartition $photon_cmdline $systemd_cmdline

Add "fips=1" to the end of the line so it reads as follows:

linux /boot/$photon_linux root=$rootpartition $photon_cmdline $systemd_cmdline fips=1

Note: Do not copy/paste in this example argument line. This may change in future releases. Find the similar line and append "fips=1" to it.

Reboot the system for the change to take effect.

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

1.52 PHTN-40-000175 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-258851
RULE ID: SV-258851r991580
```

Rationale:

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

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

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

At the command line, run the following command to verify an audit rule exists to audit kernel modules:

auditctl -l | grep init_module

Expected result:

-a always,exit -F arch=b32 -S init_module -F key=modules -a always,exit -F arch=b64 -S init_module -F key=modules

If the output does not match the expected result, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-a always,exit -F arch=b32 -S init_module -F key=modules -a always,exit -F arch=b64 -S init_module -F key=modules

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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

1.53 PHTN-40-000184 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must prevent the use of dictionary words for passwords.

```
GROUP ID: V-258853
RULE ID: SV-258853r991587
```

Rationale:

If the operating system allows the user to select passwords based on dictionary words, then this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

Audit:

At the command line, run the following command to verify passwords do not match dictionary words:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "dictcheck" option is not set to 1, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "dictcheck" option set to "1" as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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 PHTN-40-000186 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must ensure audit events are flushed to disk at proper intervals.

```
GROUP ID: V-258855
RULE ID: SV-258855r991589
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one. To that end, the auditd service must be configured to start automatically and be running at all times.

Audit:

At the command line, run the following command to verify auditd is configured to flush audit events to disk regularly:

grep -E "freq|flush" /etc/audit/auditd.conf

Example result:

flush = INCREMENTAL_ASYNC freq = 50

If "flush" is not set to "INCREMENTAL_ASYNC", this is a finding. If "freq" is not set to "50", this is a finding.

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Add or update the following lines:

flush = INCREMENTAL_ASYNC freq = 50

At the command line, run the following command:

pkill -SIGHUP auditd

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 PHTN-40-000185 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt in login.defs.

```
GROUP ID: V-258854
RULE ID: SV-258854r991588
```

Rationale:

Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

Audit:

At the command line, run the following command to verify a four second delay is configured between logon attempts:

grep '^FAIL_DELAY' /etc/login.defs

Example result:

FAIL_DELAY 4

If the "FAIL_DELAY" option is not set to 4 or more, is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or update the following line:

FAIL_DELAY 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

1.56 PHTN-40-000187 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

```
GROUP ID: V-258856
RULE ID: SV-258856r991590
```

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created they do not have unnecessary access.

Audit:

At the command line, run the following command to verify the default umask configuration:

grep '^UMASK' /etc/login.defs

Expected result:

UMASK 077

If the "UMASK" option is not set to "077", is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or update the following 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

1.57 PHTN-40-000188 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must configure Secure Shell (SSH) to disallow HostbasedAuthentication.

```
GROUP ID: V-258857
RULE ID: SV-258857r991591
```

Rationale:

SSH trust relationships enable trivial lateral spread after a host compromise and therefore must be explicitly disabled.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i HostbasedAuthentication

Example result:

hostbasedauthentication no

If "HostbasedAuthentication" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "HostbasedAuthentication" line is uncommented and set to the following:

HostbasedAuthentication no

At the command line, run the following command:

systemctl restart sshd.service

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 PHTN-40-000192 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to use the pam_faillock.so module.

```
GROUP ID: V-258858
RULE ID: SV-258858r958388
```

Rationale:

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

This module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than deny consecutive failed authentications.

Audit:

At the command line, run the following commands to verify the pam_faillock.so module is used:

grep '^auth' /etc/pam.d/system-auth

Example result:

auth required pam_faillock.so preauth auth required pam_unix.so auth required pam_faillock.so authfail

If the pam_faillock.so module is not present with the "preauth" line listed before pam_unix.so, this is a finding. If the pam_faillock.so module is not present with the "authfail" line listed after pam_unix.so, this is a finding.

grep '^account' /etc/pam.d/system-account

Example result:

account required pam_faillock.so account required pam_unix.so

If the pam_faillock.so module is not present and listed before pam_unix.so, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-auth

Add or update the following lines making sure to place the preauth line before the pam_unix.so module:

auth required pam_faillock.so preauth auth required pam_faillock.so authfail

Navigate to and open:

/etc/pam.d/system-account

Add or update the following lines making sure to place the line before the pam_unix.so module:

account required pam_faillock.so

Note: The lines shown assume the /etc/security/faillock.conf file is used to configure pam_faillock.

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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

1.59 PHTN-40-000193 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must prevent leaking information of the existence of a user account.

```
GROUP ID: V-258859
RULE ID: SV-258859r958388
```

Rationale:

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

If the pam_faillock.so module is not configured to use the silent flag it could leak information about the existence or nonexistence of a user account.

Audit:

At the command line, run the following command to verify account information is not leaked during the login process:

grep '^silent' /etc/security/faillock.conf

Example result:

silent

If the "silent" option is not set, is missing or commented out, this is a finding.

Note: If faillock.conf is not used to configure pam_faillock.so then these options may be specified on the faillock lines in the system-auth and system-account files.

Remediation:

Navigate to and open:

/etc/security/faillock.conf

Add or update the following lines:

silent

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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

1.60 PHTN-40-000194 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit logon attempts for unknown users.

```
GROUP ID: V-258860
RULE ID: SV-258860r958388
```

Rationale:

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

Audit:

At the command line, run the following command to verify that audit logon attempts for unknown users is performed:

grep '^audit' /etc/security/faillock.conf

Example result:

audit

If the "audit" option is not set, is missing or commented out, this is a finding.

Note: If faillock.conf is not used to configure pam_faillock.so then these options may be specified on the faillock lines in the system-auth and system-account files.

Remediation:

Navigate to and open:

/etc/security/faillock.conf

Add or update the following lines:

audit

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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

1.61 PHTN-40-000195 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-258861
RULE ID: SV-258861r958388
```

Rationale:

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

Unless specified the root account is not included in the default faillock module options and should be included.

Audit:

At the command line, run the following command to verify accounts are locked after three consecutive invalid logon attempts by a user during a 15-minute time period includes the root account:

grep '^even_deny_root' /etc/security/faillock.conf

Example result:

even_deny_root

If the "even_deny_root" option is not set, is missing or commented out, this is a finding.

Note: If faillock.conf is not used to configure pam_faillock.so then these options may be specified on the faillock lines in the system-auth and system-account files.

Remediation:

Navigate to and open:

/etc/security/faillock.conf

Add or update the following lines:

even_deny_root

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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

1.62 PHTN-40-000196 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must persist lockouts between system reboots.

```
GROUP ID: V-258862
RULE ID: SV-258862r1003649
```

Rationale:

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

By default, account lockout information is stored under /var/run/faillock and is not persistent between reboots.

Audit:

At the command line, run the following command to verify account locking persists lockouts between system reboots

grep '^dir' /etc/security/faillock.conf

Example result:

dir = /var/log/faillock

If the "dir" option is set to "/var/run/faillock", this is a finding. If the "dir" option is not set to a persistent documented faillock directory, is missing or commented out, this is a finding.

Note: If faillock.conf is not used to configure pam_faillock.so, these options may be specified on the faillock lines in the system-auth and system-account files.

Remediation:

Navigate to and open:

/etc/security/faillock.conf

Add or update the following lines:

dir = /var/log/faillock

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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

1.63 PHTN-40-000197 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to use the pam_pwquality.so module.

```
GROUP ID: V-258863
RULE ID: SV-258863r1003650
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

At the command line, run the following command to verify the pam_pwquality.so module is used:

grep '^password' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1 password required pam_pwhistory.so remember=5 retry=3 enforce_for_root use_authtok password required pam_unix.so sha512 use_authtok shadow try_first_pass

If the pam_pwquality.so module is not present, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add or update the pam_pwquality.so module line as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: The line must be configured before pam_pwhistory.so.

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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)

1.64 PHTN-40-000199 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system TDNF package management tool must cryptographically verify the authenticity of all software packages during installation for all repos.

```
GROUP ID: V-258864
RULE ID: SV-258864r1003651
```

Rationale:

Installation of any nontrusted software, patches, service packs, device drivers, or operating system components can significantly affect the overall security of the operating system. This requirement ensures the software has not been tampered with and has been provided by a trusted vendor.

Audit:

At the command line, run the following command to verify software packages are cryptographically verified during installation:

grep gpgcheck /etc/yum.repos.d/*

If "gpgcheck" is not set to "1" in any returned file, this is a finding.

Remediation:

Open the file where "gpgcheck" is not set to 1 with a text editor.

Add or update the following line:

gpgcheck=1

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

1.65 PHTN-40-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure the Secure Shell (SSH) SyslogFacility.

```
GROUP ID: V-258865
RULE ID: SV-258865r1003652
```

Rationale:

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and ensure ongoing compliance with remote access policies by auditing connection activities.

Shipping SSH authentication events to syslog allows organizations to use their log aggregators to correlate forensic activities among multiple systems.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i SyslogFacility

Example result:

syslogfacility AUTHPRIV

If "syslogfacility" is not set to "AUTH" or "AUTHPRIV", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "SyslogFacility" line is uncommented and set to the following:

SyslogFacility AUTHPRIV

At the command line, run the following command:

systemctl restart sshd.service

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)

1.66 PHTN-40-000201 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enable Secure Shell (SSH) authentication logging.

```
GROUP ID: V-258866
RULE ID: SV-258866r958406
```

Rationale:

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and ensure ongoing compliance with remote access policies by auditing connection activities.

The INFO LogLevel is required, at least, to ensure the capturing of failed login events.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i LogLevel

Example result:

loglevel INFO

If "LogLevel" is not set to "INFO", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "LogLevel" line is uncommented and set to the following:

LogLevel INFO

At the command line, run the following command:

systemctl restart sshd.service

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)

1.67 PHTN-40-000203 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must terminate idle Secure Shell (SSH) sessions.

```
GROUP ID: V-258867
RULE ID: SV-258867r970703
```

Rationale:

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

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level, and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i ClientAliveCountMax

Expected result:

clientalivecountmax 0

If "ClientAliveCountMax" is not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "ClientAliveCountMax" line is uncommented and set to the following:

ClientAliveCountMax 0

At the command line, run the following command:

systemctl restart sshd.service

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

1.68 PHTN-40-000204 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account modifications.

```
GROUP ID: V-258868
RULE ID: SV-258868r991551
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to modify an existing account. Auditing account modification actions provides logging that can be used for forensic purposes.

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

Satisfies: SRG-OS-000239-GPOS-00089, SRG-OS-000303-GPOS-00120, SRG-OS-000467-GPOS-00211

Audit:

At the command line, run the following command to verify an audit rule exists to audit account modifications:

auditctl -l | grep -E "(/etc/passwd|/etc/shadow|/etc/group|/etc/gshadow)"

Expected result:

-w /etc/passwd -p wa -k passwd -w /etc/shadow -p wa -k shadow -w /etc/group -p wa -k group -w /etc/gshadow -p wa -k gshadow

If the output does not match the expected result, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-w /etc/passwd -p wa -k passwd -w /etc/shadow -p wa -k shadow -w /etc/group -p wa -k group -w /etc/gshadow -p wa -k gshadow

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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

CCI-001403 Automatically audit account modification actions.

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

CCI-002130 Automatically audit account enabling actions.

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

1.69 PHTN-40-000206 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-258869
RULE ID: SV-258869r1003654
```

Rationale:

Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

Audit:

At the command line, run the following command to verify the pam_faildelay.so module is used:

grep '^auth' /etc/pam.d/system-auth

Example result:

auth required pam_faillock.so preauth auth required pam_unix.so auth required pam_faillock.so authfail auth optional pam_faildelay.so delay=4000000

If the pam_faildelay.so module is not present with the delay set to at least four seconds, this is a finding.

Note: The delay is configured in microseconds.

Remediation:

Navigate to and open:

/etc/pam.d/system-auth

Add or update the following line:

auth optional pam_faildelay.so delay=4000000

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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 PHTN-40-000207 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must configure Secure Shell (SSH) to disallow authentication with an empty password.

```
GROUP ID: V-258870
RULE ID: SV-258870r991591
```

Rationale:

Blank passwords are one of the first things an attacker checks for when probing a system. Even if the user somehow has a blank password on the OS, SSH must not allow that user to log in.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i PermitEmptyPasswords

Example result:

permitemptypasswords no

If "PermitEmptyPasswords" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "PermitEmptyPasswords" line is uncommented and set to the following:

PermitEmptyPasswords no

At the command line, run the following command:

systemctl restart sshd.service

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 PHTN-40-000208 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must configure Secure Shell (SSH) to disable user environment processing.

```
GROUP ID: V-258871
RULE ID: SV-258871r991591
```

Rationale:

Enabling user environment processing may enable users to bypass access restrictions in some configurations and must therefore be disabled.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i PermitUserEnvironment

Example result:

permituserenvironment no

If "PermitUserEnvironment" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "PermitUserEnvironment" line is uncommented and set to the following:

PermitUserEnvironment no

At the command line, run the following command:

systemctl restart sshd.service

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 PHTN-40-000209 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must create a home directory for all new local interactive user accounts.

```
GROUP ID: V-258872
RULE ID: SV-258872r991589
```

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

At the command line, run the following command to verify a home directory is created for all new user accounts:

grep '^CREATE_HOME' /etc/login.defs

Example result:

CREATE_HOME yes

If the "CREATE_HOME" option is not set to "yes", is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or update the following line:

CREATE_HOME 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

1.73 PHTN-40-000211 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to disallow Generic Security Service Application Program Interface (GSSAPI) authentication.

```
GROUP ID: V-258874
RULE ID: SV-258874r991589
```

Rationale:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through Secure Shell (SSH) exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i GSSAPIAuthentication

Example result:

gssapiauthentication no

If "GSSAPIAuthentication" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "GSSAPIAuthentication" line is uncommented and set to the following:

GSSAPIAuthentication no

At the command line, run the following command:

systemctl restart sshd.service

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

1.74 PHTN-40-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must disable the debug-shell service.

```
GROUP ID: V-258873
RULE ID: SV-258873r991589
```

Rationale:

The debug-shell service is intended to diagnose systemd related boot issues with various systemctl commands. Once enabled and following a system reboot, the root shell will be available on tty9. This service must remain disabled until and unless otherwise directed by VMware support.

Audit:

At the command line, run the following command to verify the debug-shell service is disabled:

systemctl status debug-shell.service

If the debug-shell service is not stopped and disabled, this is a finding.

Remediation:

At the command line, run the following commands:

systemctl stop debug-shell.service systemctl disable debug-shell.service

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

1.75 PHTN-40-000212 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to disable X11 forwarding.

```
GROUP ID: V-258875
RULE ID: SV-258875r991589
```

Rationale:

X11 is an older, insecure graphics forwarding protocol. It is not used by Photon and should be disabled as a general best practice to limit attack surface area and communication channels.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i X11Forwarding

Example result:

x11forwarding no

If "X11Forwarding" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "X11Forwarding" line is uncommented and set to the following:

X11Forwarding no

At the command line, run the following command:

systemctl restart sshd.service

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

1.76 PHTN-40-000213 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to perform strict mode checking of home directory configuration files.

```
GROUP ID: V-258876
RULE ID: SV-258876r991589
```

Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i StrictModes

Example result:

strictmodes yes

If "StrictModes" is not set to "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "StrictModes" line is uncommented and set to the following:

StrictModes yes

At the command line, run the following command:

systemctl restart sshd.service

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

1.77 PHTN-40-000214 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to disallow Kerberos authentication.

```
GROUP ID: V-258877
RULE ID: SV-258877r991589
```

Rationale:

If Kerberos is enabled through SSH, sshd provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i KerberosAuthentication

Example result:

kerberosauthentication no

If "KerberosAuthentication" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "KerberosAuthentication" line is uncommented and set to the following:

KerberosAuthentication no

At the command line, run the following command:

systemctl restart sshd.service

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

1.78 PHTN-40-000215 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to disallow compression of the encrypted session stream.

```
GROUP ID: V-258878
RULE ID: SV-258878r991589
```

Rationale:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i Compression

Example result:

compression no

If there is no output or if "Compression" is not set to "delayed" or "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "Compression" line is uncommented and set to the following:

Compression no

At the command line, run the following command:

systemctl restart sshd.service

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

1.79 PHTN-40-000216 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to display the last login immediately after authentication.

```
GROUP ID: V-258879
RULE ID: SV-258879r991589
```

Rationale:

Providing users with feedback on the last time they logged on via SSH facilitates user recognition and reporting of unauthorized account use.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i PrintLastLog

Example result:

printlastlog yes

If "PrintLastLog" is not set to "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "PrintLastLog" line is uncommented and set to the following:

PrintLastLog yes

At the command line, run the following command:

systemctl restart sshd.service

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

1.80 PHTN-40-000217 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to ignore user-specific trusted hosts lists.

```
GROUP ID: V-258880
RULE ID: SV-258880r991589
```

Rationale:

SSH trust relationships enable trivial lateral spread after a host compromise and therefore must be explicitly disabled. Individual users can have a local list of trusted remote machines, which must also be ignored while disabling host-based authentication generally.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i IgnoreRhosts

Example result:

ignorerhosts yes

If "IgnoreRhosts" is not set to "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "IgnoreRhosts" line is uncommented and set to the following:

IgnoreRhosts yes

At the command line, run the following command:

systemctl restart sshd.service

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

1.81 PHTN-40-000218 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to ignore user-specific known_host files.

```
GROUP ID: V-258881
RULE ID: SV-258881r991589
```

Rationale:

SSH trust relationships enable trivial lateral spread after a host compromise and therefore must be explicitly disabled. Individual users can have a local list of trusted remote machines, which must also be ignored while disabling host-based authentication generally.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i IgnoreUserKnownHosts

Expected result:

ignoreuserknownhosts yes

If "IgnoreUserKnownHosts" is not set to "yes", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "IgnoreUserKnownHosts" line is uncommented and set to the following:

IgnoreUserKnownHosts yes

At the command line, run the following command:

systemctl restart sshd.service

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

1.82 PHTN-40-000219 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to limit the number of allowed login attempts per connection.

```
GROUP ID: V-258882
RULE ID: SV-258882r991589
```

Rationale:

By setting the login attempt limit to a low value, an attacker will be forced to reconnect frequently, which severely limits the speed and effectiveness of brute-force attacks.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i MaxAuthTries

Example result:

maxauthtries 6

If "MaxAuthTries" is not set to "6", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "MaxAuthTries" line is uncommented and set to the following:

MaxAuthTries 6

At the command line, run the following command:

systemctl restart sshd.service

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 PHTN-40-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to restrict AllowTcpForwarding.

```
GROUP ID: V-258883
RULE ID: SV-258883r991589
```

Rationale:

While enabling TCP tunnels is a valuable function of sshd, this feature is not appropriate for use on single purpose appliances.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i AllowTcpForwarding

Example result:

allowtcpforwarding no

If "AllowTcpForwarding" is not set to "no", this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "AllowTcpForwarding" line is uncommented and set to the following:

AllowTcpForwarding no

At the command line, run the following command:

systemctl restart sshd.service

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 PHTN-40-000221 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure Secure Shell (SSH) to restrict LoginGraceTime.

```
GROUP ID: V-258884
RULE ID: SV-258884r991589
```

Rationale:

By default, SSH unauthenticated connections are left open for two minutes before being closed. This setting is too permissive as no legitimate login would need such an amount of time to complete a login. Quickly terminating idle or incomplete login attempts will free up resources and reduce the exposure any partial logon attempts may create.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i LoginGraceTime

Example result:

logingracetime 30

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

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "LoginGraceTime" line is uncommented and set to the following:

LoginGraceTime 30

At the command line, run the following command:

systemctl restart sshd.service

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

1.85 PHTN-40-000222 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled on the command line.

```
GROUP ID: V-258885
RULE ID: SV-258885r991589
```

Rationale:

When the Ctrl-Alt-Del target is enabled, a locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of systems availability due to unintentional reboot.

Audit:

At the command line, run the following command to verify the ctrl-alt-del target is disabled and masked:

systemctl status ctrl-alt-del.target --no-pager

Example output:

ctrl-alt-del.target Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.) Active: inactive (dead)

If the "ctrl-alt-del.target" is not "inactive" and "masked", this is a finding.

Remediation:

At the command line, run the following commands:

systemctl disable ctrl-alt-del.target systemctl mask ctrl-alt-del.target systemctl daemon-reload

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

1.86 PHTN-40-000223 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not forward IPv4 or IPv6 source-routed packets.

```
GROUP ID: V-258886
RULE ID: SV-258886r991589
```

Rationale:

Source routing is an Internet Protocol mechanism that allows an IP packet to carry information, a list of addresses, that tells a router the path the packet must take. There is also an option to record the hops as the route is traversed.

The list of hops taken, the "route record", provides the destination with a return path to the source. This allows the source (the sending host) to specify the route, loosely or strictly, ignoring the routing tables of some or all of the routers. It can allow a user to redirect network traffic for malicious purposes and should therefore be disabled.

Audit:

At the command line, run the following command to verify source-routed packets are not forwarded:

/sbin/sysctl -a --pattern "net.ipv[4|6].conf.(all|default).accept_source_route"

Expected result:

net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

If the "accept_source_route" kernel parameters are not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following lines:

net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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 PHTN-40-000224 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not respond to IPv4 Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

```
GROUP ID: V-258887
RULE ID: SV-258887r991589
```

Rationale:

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Audit:

At the command line, run the following command to verify ICMP echoes sent to a broadcast address are ignored:

/sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts

Example result:

net.ipv4.icmp_echo_ignore_broadcasts = 1

If the "net.ipv4.icmp_echo_ignore_broadcasts" kernel parameter is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

net.ipv4.icmp_echo_ignore_broadcasts = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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

1.88 PHTN-40-000225 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-258888
RULE ID: SV-258888r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

At the command line, run the following command to verify ICMP redirects are not accepted:

/sbin/sysctl -a --pattern "net.ipv4.conf.(all|default).accept_redirects"

Expected result:

net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0

If the "accept_redirects" kernel parameters are not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following lines:

net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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

1.89 PHTN-40-000226 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must prevent IPv4 Internet Control Message Protocol (ICMP) secure redirect messages from being accepted.

```
GROUP ID: V-258889
RULE ID: SV-258889r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

At the command line, run the following command to verify ICMP secure redirects are not accepted:

/sbin/sysctl -a --pattern "net.ipv4.conf.(all|default).secure_redirects"

Expected result:

net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0

If the "secure_redirects" kernel parameters are not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following lines:

net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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 PHTN-40-000227 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not send IPv4 Internet Control Message Protocol (ICMP) redirects.

```
GROUP ID: V-258890
RULE ID: SV-258890r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

Audit:

At the command line, run the following command to verify ICMP send redirects are not accepted:

/sbin/sysctl -a --pattern "net.ipv4.conf.(all|default).send_redirects"

Expected result:

net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0

If the "send_redirects" kernel parameters are not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following lines:

net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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

1.91 PHTN-40-000228 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must log IPv4 packets with impossible addresses.

```
GROUP ID: V-258891
RULE ID: SV-258891r991589
```

Rationale:

The presence of "martian" packets (which have impossible addresses) as well as spoofed packets, source-routed packets, and redirects could be a sign of nefarious network activity. Logging these packets enables this activity to be detected.

Audit:

At the command line, run the following command to verify martian packets are logged:

/sbin/sysctl -a --pattern "net.ipv4.conf.(all|default).log_martians"

Expected result:

net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1

If the "log_martians" kernel parameters are not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following lines:

net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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

1.92 PHTN-40-000229 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must use a reverse-path filter for IPv4 network traffic.

```
GROUP ID: V-258892
RULE ID: SV-258892r991589
```

Rationale:

Enabling reverse path filtering drops packets with source addresses that should not have been able to be received on the interface they were received on. It should not be used on systems that are routers for complicated networks but is helpful for end hosts and routers serving small networks.

Audit:

At the command line, run the following command to verify IPv4 traffic is using a reverse path filter:

/sbin/sysctl -a --pattern "net.ipv4.conf.(all|default).rp_filter"

Expected result:

net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1

If the "rp_filter" kernel parameters are not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following lines:

net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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 PHTN-40-000231 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not perform IPv4 packet forwarding.

```
GROUP ID: V-258893
RULE ID: SV-258893r991589
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Audit:

If IP forwarding is required, for example if Kubernetes is installed, this is Not Applicable.

At the command line, run the following command to verify packet forwarding it disabled:

/sbin/sysctl net.ipv4.ip_forward

Expected result:

net.ipv4.ip_forward = 0

If the "net.ipv4.ip_forward" kernel parameter is not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

net.ipv4.ip_forward = 0

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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 PHTN-40-000232 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must send TCP timestamps.

```
GROUP ID: V-258894
RULE ID: SV-258894r991589
```

Rationale:

TCP timestamps are used to provide protection against wrapped sequence numbers. It is possible to calculate system uptime (and boot time) by analyzing TCP timestamps. These calculated uptimes can help a bad actor in determining likely patch levels for vulnerabilities.

Audit:

At the command line, run the following command to verify TCP timestamps are enabled:

/sbin/sysctl net.ipv4.tcp_timestamps

Expected result:

net.ipv4.tcp_timestamps = 1

If the "net.ipv4.tcp_timestamps" kernel parameter is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

net.ipv4.tcp_timestamps = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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 PHTN-40-000233 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to protect the Secure Shell (SSH) public host key from unauthorized modification.

```
GROUP ID: V-258895
RULE ID: SV-258895r991589
```

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

At the command line, run the following command:

stat -c "%n permissions are %a and owned by %U:%G" /etc/ssh/*key.pub

Example result:

/etc/ssh/ssh_host_dsa_key.pub permissions are 644 and owned by root:root
/etc/ssh/ssh_host_ecdsa_key.pub permissions are 644 and owned by root:root
/etc/ssh/ssh_host_ed25519_key.pub permissions are 644 and owned by root:root
/etc/ssh/ssh_host_rsa_key.pub permissions are 644 and owned by root:root

If any "key.pub" file listed is not owned by root or not group owned by root or does not have permissions of "0644", this is a finding.

Remediation:

At the command line, run the following commands for each returned file:

chmod 644 chown root:root systemctl restart sshd.service

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

1.96 PHTN-40-000234 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to protect the Secure Shell (SSH) private host key from unauthorized access.

```
GROUP ID: V-258896
RULE ID: SV-258896r991589
```

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Audit:

At the command line, run the following command:

stat -c "%n permissions are %a and owned by %U:%G" /etc/ssh/*key

Example result:

/etc/ssh/ssh_host_dsa_key permissions are 600 and owned by root:root
/etc/ssh/ssh_host_ecdsa_key permissions are 600 and owned by root:root
/etc/ssh/ssh_host_ed25519_key permissions are 600 and owned by root:root
/etc/ssh/ssh_host_rsa_key permissions are 600 and owned by root:root

If any key file listed is not owned by root or not group owned by root or does not have permissions of "0600", this is a finding.

Remediation:

At the command line, run the following commands for each returned file:

chmod 600 chown root:root systemctl restart sshd.service

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 PHTN-40-000235 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce password complexity on the root account.

```
GROUP ID: V-258897
RULE ID: SV-258897r991589
```

Rationale:

Password complexity rules must apply to all accounts on the system, including root. Without specifying the enforce_for_root flag, pam_pwquality does not apply complexity rules to the root user. While root users can find ways around this requirement, given its superuser power, it is necessary to attempt to force compliance.

Audit:

At the command line, run the following command to verify password complexity is enforced for the root account:

grep '^password.*pam_pwquality.so' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

If the "enforce_for_root" option is missing or commented out, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Configure the pam_pwquality.so line to have the "enforce_for_root" option present as follows:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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 PHTN-40-000236 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must disable systemd fallback DNS.

```
GROUP ID: V-258898
RULE ID: SV-258898r991589
```

Rationale:

Systemd contains an ability to set fallback DNS servers, which is used for DNS lookups in the event no system level DNS servers are configured or other DNS servers are specified in the Systemd resolved.conf file. If uncommented, this configuration contains Google DNS servers by default and could result in DNS leaking info unknowingly in the event DNS is absent or misconfigured at the system level.

Audit:

At the command line, run the following command to verify systemd fallback DNS is disabled:

resolvectl status | grep '^Fallback DNS'

If the output indicates that Fallback DNS servers are configured, this is a finding.

Remediation:

Navigate to and open:

/etc/systemd/resolved.conf

Add or update the "FallbackDNS" entry to the following:

FallbackDNS=

Restart the Systemd resolved service by running the following command:

systemctl restart systemd-resolved

Note: If this option is not given, a compiled-in list of DNS servers is used instead, which is undesirable.

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 PHTN-40-000237 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure AIDE to detect changes to baseline configurations.

```
GROUP ID: V-266062
RULE ID: SV-266062r1003658
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's information system security manager (ISSM)/information system security officer (ISSO) and system administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Audit:

At the command line, run the following commands to verify AIDE is configured and used to monitor for file changes:

grep -v '^' /etc/aide.conf | grep -v '^$'

Example result:

STIG = p+i+n+u+g+s+m+S LOGS = p+n+u+g /boot STIG /opt STIG /usr STIG /etc STIG /var/log LOGS

If the AIDE configuration does not include the lines shown above, this is a finding.

At the command line, run the following commands to verify an AIDE database is configured and used to monitor for file changes:

aide --check

If the check command indicates there is no database available, this is a finding.

Remediation:

Update the /etc/aide.conf file with the template provided as a supplemental document.

At the command line, run the following commands to generate an AIDE database to use for file monitoring:

aide --init cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Note: It is recommended to run these fix steps after all other STIG configurations have been completed so that the AIDE database includes those updates.

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)

1.100 PHTN-40-000238 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must generate audit records for all access and modifications to the opasswd file.

```
GROUP ID: V-258899
RULE ID: SV-258899r991589
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

At the command line, run the following command to verify an audit rule exists to audit the opasswd file:

auditctl -l | grep -E /etc/security/opasswd

Expected result:

-w /etc/security/opasswd -p wa -k opasswd

If the opasswd file is not monitored for access or writes, this is a finding.

Note: This check depends on the "auditd" service to be in a running state for accurate results. The "auditd" service is enabled in control PHTN-40-000016.

Remediation:

Navigate to and open:

/etc/audit/rules.d/audit.STIG.rules

Add or update the following lines:

-w /etc/security/opasswd -p wa -k opasswd

At the command line, run the following command to load the new audit rules:

/sbin/augenrules --load

Note: An "audit.STIG.rules" file is provided with this guidance for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist and may reference older "GEN" SRG IDs. This file can be removed and replaced as necessary with an updated one.

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 PHTN-40-000239 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Photon operating system must implement only approved Message Authentication Codes (MACs) to protect the integrity of remote access sessions.

```
GROUP ID: V-258900
RULE ID: SV-258900r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Audit:

At the command line, run the following command to verify the running configuration of sshd:

sshd -T|&grep -i MACs

Example result:

macs hmac-sha2-512,hmac-sha2-256

If the output matches the macs in the example result or a subset thereof, this is not a finding.

If the output contains any macs not listed in the example result, this is a finding.

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

Ensure the "MACs" line is uncommented and set to the following:

MACs hmac-sha2-512,hmac-sha2-256

At the command line, run the following command:

systemctl restart sshd.service

Additional Information:

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)

1.102 PHTN-40-000242 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enable the rsyslog service.

```
GROUP ID: V-258901
RULE ID: SV-258901r991589
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration. Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

If another package is used to offload logs, such as syslog-ng, and is properly configured, this is not applicable.

At the command line, run the following command to verify rsyslog is enabled and running:

systemctl status rsyslog

If the rsyslog service is not enabled and running, this is a finding.

Remediation:

At the command line, run the following commands:

systemctl enable rsyslog systemctl start rsyslog

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 PHTN-40-000243 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured to use the pam_pwhistory.so module.

```
GROUP ID: V-258902
RULE ID: SV-258902r1003655
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

Audit:

At the command line, run the following command to verify the pam_pwhistory.so module is used:

grep '^password' /etc/pam.d/system-password

Example result:

password requisite pam_pwquality.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=15 difok=8 enforce_for_root dictcheck=1 password required pam_pwhistory.so remember=5 retry=3 enforce_for_root use_authtok password required pam_unix.so sha512 use_authtok shadow try_first_pass

If the "pam_pwhistory.so" module is not present, this is a finding. If "use_authtok" is not present for the "pam_pwhistory.so" module, this is a finding. If "conf" or "file" are present for the "pam_pwhistory.so" module, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add or update the pam_pwhistory.so module line as follows:

password required pam_pwhistory.so remember=5 retry=3 enforce_for_root use_authtok

Note: The line must be configured after pam_pwquality.so.

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

Additional Information:

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

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

1.104 PHTN-40-000244 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enable hardlink access control protection in the kernel.

```
GROUP ID: V-258903
RULE ID: SV-258903r991589
```

Rationale:

By enabling the fs.protected_hardlinks kernel parameter, users can no longer create soft or hard links to files they do not own. Disallowing such hardlinks mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Audit:

At the command line, run the following command to verify hardlink protection is enabled:

/sbin/sysctl fs.protected_hardlinks

Example result:

fs.protected_hardlinks = 1

If the "fs.protected_hardlinks" kernel parameter is not set to "1", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

fs.protected_hardlinks = 1

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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

1.105 PHTN-40-000246 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must restrict core dumps.

```
GROUP ID: V-258904
RULE ID: SV-258904r991589
```

Rationale:

By enabling the fs.suid_dumpable kernel parameter, core dumps are not generated for setuid or otherwise protected/tainted binaries. This prevents users from potentially accessing core dumps with privileged information they would otherwise not have access to read.

Audit:

At the command line, run the following command to verify core dumps are restricted:

/sbin/sysctl fs.suid_dumpable

Example result:

fs.suid_dumpable = 0

If the "fs.suid_dumpable" kernel parameter is not set to "0", this is a finding.

Remediation:

Navigate to and open:

/etc/sysctl.d/zz-stig-hardening.conf

Add or update the following line:

fs.suid_dumpable = 0

At the command line, run the following command to load the new configuration:

/sbin/sysctl --load /etc/sysctl.d/zz-stig-hardening.conf

Note: If the file zz-stig-hardening.conf does not exist, it must be created.

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 PHTN-40-000247 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not allow empty passwords.

```
GROUP ID: V-266063
RULE ID: SV-266063r1003661
```

Rationale:

Accounts with empty or no passwords allow anyone to log on as that account without specifying a password or other forms of authentication. Allowing accounts with empty passwords puts the system at significant risk since only the username is required for access.

Audit:

At the command line, run the following command to verify empty passwords are not allowed:

grep nullok /etc/pam.d/system-password /etc/pam.d/system-auth

If any results are returned indicating "nullok" is configured on the "pam_unix.so" module, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password or /etc/pam.d/system-auth

Remove the "nullok" argument on the "pam_unix.so" module line.

Note: On vCenter appliances, the equivalent file must be edited under "/etc/applmgmt/appliance", if one exists, for the changes to persist after a reboot.

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	PHTN-40-000003 (Manual)	☐	☐
1.2	PHTN-40-000004 (Manual)	☐	☐
1.3	PHTN-40-000007 (Manual)	☐	☐
1.4	PHTN-40-000005 (Manual)	☐	☐
1.5	PHTN-40-000012 (Manual)	☐	☐
1.6	PHTN-40-000013 (Manual)	☐	☐
1.7	PHTN-40-000014 (Manual)	☐	☐
1.8	PHTN-40-000016 (Manual)	☐	☐
1.9	PHTN-40-000021 (Manual)	☐	☐
1.10	PHTN-40-000019 (Manual)	☐	☐
1.11	PHTN-40-000026 (Manual)	☐	☐
1.12	PHTN-40-000030 (Manual)	☐	☐
1.13	PHTN-40-000031 (Manual)	☐	☐
1.14	PHTN-40-000035 (Manual)	☐	☐
1.15	PHTN-40-000036 (Manual)	☐	☐
1.16	PHTN-40-000037 (Manual)	☐	☐
1.17	PHTN-40-000038 (Manual)	☐	☐
1.18	PHTN-40-000039 (Manual)	☐	☐
1.19	PHTN-40-000040 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	PHTN-40-000041 (Manual)	☐	☐
1.21	PHTN-40-000042 (Manual)	☐	☐
1.22	PHTN-40-000043 (Manual)	☐	☐
1.23	PHTN-40-000044 (Manual)	☐	☐
1.24	PHTN-40-000046 (Manual)	☐	☐
1.25	PHTN-40-000047 (Manual)	☐	☐
1.26	PHTN-40-000049 (Manual)	☐	☐
1.27	PHTN-40-000059 (Manual)	☐	☐
1.28	PHTN-40-000067 (Manual)	☐	☐
1.29	PHTN-40-000068 (Manual)	☐	☐
1.30	PHTN-40-000069 (Manual)	☐	☐
1.31	PHTN-40-000073 (Manual)	☐	☐
1.32	PHTN-40-000074 (Manual)	☐	☐
1.33	PHTN-40-000076 (Manual)	☐	☐
1.34	PHTN-40-000078 (Manual)	☐	☐
1.35	PHTN-40-000079 (Manual)	☐	☐
1.36	PHTN-40-000080 (Manual)	☐	☐
1.37	PHTN-40-000082 (Manual)	☐	☐
1.38	PHTN-40-000086 (Manual)	☐	☐
1.39	PHTN-40-000092 (Manual)	☐	☐
1.40	PHTN-40-000093 (Manual)	☐	☐
1.41	PHTN-40-000105 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	PHTN-40-000107 (Manual)	☐	☐
1.43	PHTN-40-000108 (Manual)	☐	☐
1.44	PHTN-40-000110 (Manual)	☐	☐
1.45	PHTN-40-000112 (Manual)	☐	☐
1.46	PHTN-40-000130 (Manual)	☐	☐
1.47	PHTN-40-000133 (Manual)	☐	☐
1.48	PHTN-40-000160 (Manual)	☐	☐
1.49	PHTN-40-000161 (Manual)	☐	☐
1.50	PHTN-40-000173 (Manual)	☐	☐
1.51	PHTN-40-000182 (Manual)	☐	☐
1.52	PHTN-40-000175 (Manual)	☐	☐
1.53	PHTN-40-000184 (Manual)	☐	☐
1.54	PHTN-40-000186 (Manual)	☐	☐
1.55	PHTN-40-000185 (Manual)	☐	☐
1.56	PHTN-40-000187 (Manual)	☐	☐
1.57	PHTN-40-000188 (Manual)	☐	☐
1.58	PHTN-40-000192 (Manual)	☐	☐
1.59	PHTN-40-000193 (Manual)	☐	☐
1.60	PHTN-40-000194 (Manual)	☐	☐
1.61	PHTN-40-000195 (Manual)	☐	☐
1.62	PHTN-40-000196 (Manual)	☐	☐
1.63	PHTN-40-000197 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	PHTN-40-000199 (Manual)	☐	☐
1.65	PHTN-40-000200 (Manual)	☐	☐
1.66	PHTN-40-000201 (Manual)	☐	☐
1.67	PHTN-40-000203 (Manual)	☐	☐
1.68	PHTN-40-000204 (Manual)	☐	☐
1.69	PHTN-40-000206 (Manual)	☐	☐
1.70	PHTN-40-000207 (Manual)	☐	☐
1.71	PHTN-40-000208 (Manual)	☐	☐
1.72	PHTN-40-000209 (Manual)	☐	☐
1.73	PHTN-40-000211 (Manual)	☐	☐
1.74	PHTN-40-000210 (Manual)	☐	☐
1.75	PHTN-40-000212 (Manual)	☐	☐
1.76	PHTN-40-000213 (Manual)	☐	☐
1.77	PHTN-40-000214 (Manual)	☐	☐
1.78	PHTN-40-000215 (Manual)	☐	☐
1.79	PHTN-40-000216 (Manual)	☐	☐
1.80	PHTN-40-000217 (Manual)	☐	☐
1.81	PHTN-40-000218 (Manual)	☐	☐
1.82	PHTN-40-000219 (Manual)	☐	☐
1.83	PHTN-40-000220 (Manual)	☐	☐
1.84	PHTN-40-000221 (Manual)	☐	☐
1.85	PHTN-40-000222 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	PHTN-40-000223 (Manual)	☐	☐
1.87	PHTN-40-000224 (Manual)	☐	☐
1.88	PHTN-40-000225 (Manual)	☐	☐
1.89	PHTN-40-000226 (Manual)	☐	☐
1.90	PHTN-40-000227 (Manual)	☐	☐
1.91	PHTN-40-000228 (Manual)	☐	☐
1.92	PHTN-40-000229 (Manual)	☐	☐
1.93	PHTN-40-000231 (Manual)	☐	☐
1.94	PHTN-40-000232 (Manual)	☐	☐
1.95	PHTN-40-000233 (Manual)	☐	☐
1.96	PHTN-40-000234 (Manual)	☐	☐
1.97	PHTN-40-000235 (Manual)	☐	☐
1.98	PHTN-40-000236 (Manual)	☐	☐
1.99	PHTN-40-000237 (Manual)	☐	☐
1.100	PHTN-40-000238 (Manual)	☐	☐
1.101	PHTN-40-000239 (Manual)	☐	☐
1.102	PHTN-40-000242 (Manual)	☐	☐
1.103	PHTN-40-000243 (Manual)	☐	☐
1.104	PHTN-40-000244 (Manual)	☐	☐
1.105	PHTN-40-000246 (Manual)	☐	☐
1.106	PHTN-40-000247 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
09-15-2025	1.0.0	Initial CIS Release