CIS VMware vSphere 7.0 vCenter Appliance Photon OS STIG Benchmark

v1.0.0 - 08-20-2025

Terms of Use

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

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

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

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

Table of Contents

Terms of Use *1*

Table of Contents *2*

Overview *5*

Target Technology Details **5**

Intended Audience **5**

Recommendation Definitions *6*

Title **6**

Assessment Status **6**

Automated **6**

Manual **6**

Profile **6**

Description **6**

Rationale Statement **6**

Audit Procedure **6**

Remediation Procedure **7**

Additional Information **7**

Profile Definitions **8**

Acknowledgements **9**

Recommendations *10*

1 STIG RULES **10**

1.1 PHTN-30-000001 (Manual) 11
1.2 PHTN-30-000002 (Manual) 13
1.3 PHTN-30-000003 (Manual) 15
1.4 PHTN-30-000004 (Manual) 19
1.5 PHTN-30-000005 (Manual) 20
1.6 PHTN-30-000006 (Manual) 22
1.7 PHTN-30-000007 (Manual) 23
1.8 PHTN-30-000008 (Manual) 25
1.9 PHTN-30-000009 (Manual) 27
1.10 PHTN-30-000010 (Manual) 29
1.11 PHTN-30-000011 (Manual) 31
1.12 PHTN-30-000012 (Manual) 33
1.13 PHTN-30-000013 (Manual) 35
1.14 PHTN-30-000014 (Manual) 38
1.15 PHTN-30-000015 (Manual) 40
1.16 PHTN-30-000016 (Manual) 42
1.17 PHTN-30-000017 (Manual) 43
1.18 PHTN-30-000018 (Manual) 44
1.19 PHTN-30-000019 (Manual) 45
1.20 PHTN-30-000020 (Manual) 46

1.21 PHTN-30-000021 (Manual) 48
1.22 PHTN-30-000022 (Manual) 50
1.23 PHTN-30-000023 (Manual) 52
1.24 PHTN-30-000024 (Manual) 54
1.25 PHTN-30-000025 (Manual) 56
1.26 PHTN-30-000026 (Manual) 57
1.27 PHTN-30-000027 (Manual) 60
1.28 PHTN-30-000028 (Manual) 61
1.29 PHTN-30-000029 (Manual) 62
1.30 PHTN-30-000030 (Manual) 64
1.31 PHTN-30-000031 (Manual) 66
1.32 PHTN-30-000032 (Manual) 69
1.33 PHTN-30-000033 (Manual) 71
1.34 PHTN-30-000035 (Manual) 72
1.35 PHTN-30-000036 (Manual) 74
1.36 PHTN-30-000037 (Manual) 76
1.37 PHTN-30-000038 (Manual) 78
1.38 PHTN-30-000040 (Manual) 80
1.39 PHTN-30-000041 (Manual) 81
1.40 PHTN-30-000042 (Manual) 82
1.41 PHTN-30-000043 (Manual) 84
1.42 PHTN-30-000044 (Manual) 86
1.43 PHTN-30-000045 (Manual) 88
1.44 PHTN-30-000046 (Manual) 90
1.45 PHTN-30-000047 (Manual) 92
1.46 PHTN-30-000048 (Manual) 93
1.47 PHTN-30-000050 (Manual) 95
1.48 PHTN-30-000051 (Manual) 97
1.49 PHTN-30-000054 (Manual) 98
1.50 PHTN-30-000055 (Manual) 100
1.51 PHTN-30-000056 (Manual) 102
1.52 PHTN-30-000057 (Manual) 104
1.53 PHTN-30-000059 (Manual) 106
1.54 PHTN-30-000060 (Manual) 107
1.55 PHTN-30-000061 (Manual) 108
1.56 PHTN-30-000062 (Manual) 109
1.57 PHTN-30-000064 (Manual) 111
1.58 PHTN-30-000065 (Manual) 113
1.59 PHTN-30-000066 (Manual) 114
1.60 PHTN-30-000067 (Manual) 115
1.61 PHTN-30-000068 (Manual) 117
1.62 PHTN-30-000069 (Manual) 119
1.63 PHTN-30-000070 (Manual) 121
1.64 PHTN-30-000071 (Manual) 123
1.65 PHTN-30-000072 (Manual) 124
1.66 PHTN-30-000073 (Manual) 125
1.67 PHTN-30-000074 (Manual) 126
1.68 PHTN-30-000075 (Manual) 128
1.69 PHTN-30-000076 (Manual) 129
1.70 PHTN-30-000078 (Manual) 130
1.71 PHTN-30-000079 (Manual) 131
1.72 PHTN-30-000080 (Manual) 132
1.73 PHTN-30-000081 (Manual) 133
1.74 PHTN-30-000082 (Manual) 134
1.75 PHTN-30-000083 (Manual) 135
1.76 PHTN-30-000084 (Manual) 136

1.77 PHTN-30-000085 (Manual) 137
1.78 PHTN-30-000086 (Manual) 138
1.79 PHTN-30-000087 (Manual) 140
1.80 PHTN-30-000088 (Manual) 142
1.81 PHTN-30-000089 (Manual) 143
1.82 PHTN-30-000090 (Manual) 144
1.83 PHTN-30-000091 (Manual) 145
1.84 PHTN-30-000092 (Manual) 146
1.85 PHTN-30-000093 (Manual) 147
1.86 PHTN-30-000094 (Manual) 148
1.87 PHTN-30-000095 (Manual) 149
1.88 PHTN-30-000096 (Manual) 150
1.89 PHTN-30-000097 (Manual) 151
1.90 PHTN-30-000098 (Manual) 152
1.91 PHTN-30-000099 (Manual) 154
1.92 PHTN-30-000100 (Manual) 155
1.93 PHTN-30-000101 (Manual) 157
1.94 PHTN-30-000102 (Manual) 159
1.95 PHTN-30-000103 (Manual) 161
1.96 PHTN-30-000104 (Manual) 162
1.97 PHTN-30-000105 (Manual) 163
1.98 PHTN-30-000106 (Manual) 165
1.99 PHTN-30-000107 (Manual) 166
1.100 PHTN-30-000108 (Manual) 167
1.101 PHTN-30-000109 (Manual) 168
1.102 PHTN-30-000110 (Manual) 169
1.103 PHTN-30-000111 (Manual) 171
1.104 PHTN-30-000112 (Manual) 172
1.105 PHTN-30-000113 (Manual) 173
1.106 PHTN-30-000114 (Manual) 174
1.107 PHTN-30-000115 (Manual) 175
1.108 PHTN-30-000117 (Manual) 176
1.109 PHTN-30-000118 (Manual) 177
1.110 PHTN-30-000119 (Manual) 178
1.111 PHTN-30-000120 (Manual) 179
1.112 PHTN-30-000240 (Manual) 180
1.113 PHTN-30-000245 (Manual) 182

Appendix: Summary Table 184

Appendix: Change History 190

Overview

Target Technology Details

VMware vSphere 7.0 vCenter Appliance Photon OS Secure Technical Implementation Guide (STIG)

Version: 1 Release: 4 Benchmark

Date: 30 Jan 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware vSphere 7.0 vCenter Appliance Photon OS 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 7.0 vCenter Appliance Photon OS

Recommendations

1 STIG RULES

VMware vSphere 7.0

VMware vSphere 7.0 vCenter Appliance Photon OS Secure Technical Implementation Guide (STIG)

Version: 1 Release: 4 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 PHTN-30-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account creations.

```
GROUP ID: V-256478
RULE ID: SV-256478r958368
```

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.

Audit:

At the command line, run the following command:

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

Expected 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-30-000013.

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: A new "audit.STIG.rules" file is provided 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)

1.2 PHTN-30-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must automatically lock an account when three unsuccessful logon attempts occur.

```
GROUP ID: V-256479
RULE ID: SV-256479r958388
```

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.

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

Audit:

At the command line, run the following commands:

```
# grep pam_tally2 /etc/pam.d/system-auth
```

Expected result:

auth required pam_tally2.so deny=3 onerr=fail audit even_deny_root unlock_time=900 root_unlock_time=300

```
# grep pam_tally2 /etc/pam.d/system-account
```

Expected result:

account required pam_tally2.so onerr=fail audit

If the output does not list the "pam_tally2" options as configured in the expected results, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-auth

Remove any existing "pam_tally2.so" line and add the following line after the "pam_unix.so" statement:

auth required pam_tally2.so deny=3 onerr=fail audit even_deny_root unlock_time=900 root_unlock_time=300

Navigate to and open:

/etc/pam.d/system-account

Remove any existing "pam_tally2.so" line and add the following line after the "pam_unix.so" statement:

account required pam_tally2.so onerr=fail 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

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

1.3 PHTN-30-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting Secure Shell (SSH) access.

```
GROUP ID: V-256480
RULE ID: SV-256480r958390
```

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.

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

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i Banner
```

Expected result:

banner /etc/issue

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

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

1.4 PHTN-30-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

```
GROUP ID: V-256481
RULE ID: SV-256481r958398
```

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 attacks.

Audit:

At the command line, run the following command:

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

Expected result:

```
*       hard    maxlogins       10
```

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

Note: The expected result may be repeated multiple times.

Remediation:

At the command line, run the following command:

```
# echo '*       hard    maxlogins       10' >> /etc/security/limits.conf
```

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

1.5 PHTN-30-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must set a session inactivity timeout of 15 minutes or less.

```
GROUP ID: V-256482
RULE ID: SV-256482r958402
```

Rationale:

A session timeout is an action taken when a session goes idle for any reason. Rather than relying on the user to manually disconnect their session prior to going idle, the Photon operating system must be able to identify when a session has idled and take action to terminate the session.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000279-GPOS-00109, SRG-OS-000126-GPOS-00066

Audit:

At the command line, run the following command:

```
# cat /etc/profile.d/tmout.sh
```

Expected result:

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

If the file "tmout.sh" does not exist or the output does not look like the expected result, 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-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

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

CCI-000879 The organization terminates sessions and network connections when nonlocal maintenance is completed.

- NIST SP 800-53::MA-4 e
- NIST SP 800-53A::MA-4.1 (vi)
- NIST SP 800-53 Revision 4::MA-4 e

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

1.6 PHTN-30-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must have the sshd SyslogFacility set to "authpriv".

```
GROUP ID: V-256483
RULE ID: SV-256483r958406
```

Rationale:

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

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i SyslogFacility
```

Expected result:

syslogfacility AUTHPRIV

If there is no output or if the output does not match the expected result, 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)

1.7 PHTN-30-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must have sshd authentication logging enabled.

```
GROUP ID: V-256484
RULE ID: SV-256484r958406
```

Rationale:

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

Shipping sshd 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:

```
# grep "^authpriv" /etc/rsyslog.conf
```

Expected result should be similar to the following:

authpriv.* /var/log/auth.log

If "authpriv" is not configured to be logged, this is a finding.

Remediation:

Navigate to and open:

/etc/rsyslog.conf

Add the following line:

authpriv.* /var/log/auth.log

Note: The path can be substituted for another suitable log destination.

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)

1.8 PHTN-30-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must have the sshd LogLevel set to "INFO".

```
GROUP ID: V-256485
RULE ID: SV-256485r958406
```

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:

```
# sshd -T|&grep -i LogLevel
```

Expected result:

LogLevel INFO

If the output does not match the expected result, 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)

1.9 PHTN-30-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Photon operating system must configure sshd to use approved encryption algorithms.

```
GROUP ID: V-256486
RULE ID: SV-256486r958408
```

Rationale:

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

OpenSSH on the Photon operating system is compiled with a FIPS-validated cryptographic module. The "FipsMode" setting controls whether this module is initialized and used in FIPS 140-2 mode.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000393-GPOS-00173, SRG-OS-000396-GPOS-00176, SRG-OS-000250-GPOS-00093, SRG-OS-000423-GPOS-00187

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i FipsMode
```

Expected result:

FipsMode yes

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

Remediation:

Navigate to and open:

/etc/ssh/sshd_config

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

FipsMode yes

At the command line, run the following command:

```
# systemctl restart sshd.service
```

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

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

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

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

CCI-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)

1.10 PHTN-30-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256487
RULE ID: SV-256487r958412
```

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.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019

Audit:

At the command line, run the following command:

```
# grep "^write_logs" /etc/audit/auditd.conf
```

Expected result:

write_logs = yes

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

If the output does not match the expected result, 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:

```
# killproc auditd -TERM
# systemctl start 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

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

1.11 PHTN-30-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure auditd to use the correct log format.

```
GROUP ID: V-256488
RULE ID: SV-256488r958414
```

Rationale:

To compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know exact, unfiltered details of the event in question.

Audit:

At the command line, run the following command:

```
# grep "^log_format" /etc/audit/auditd.conf
```

Expected result:

log_format = RAW

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

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

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

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

log_format = RAW

At the command line, run the following command:

```
# killproc auditd -TERM
# systemctl start auditd
```

Additional Information:

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

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

1.12 PHTN-30-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256489
RULE ID: SV-256489r958422
```

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.

Audit:

At the command line, run the following command:

```
# 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. Enabling the auditd service is done in control PHTN-30-000013.

Remediation:

Navigate to and open:

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

Add 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: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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)

1.13 PHTN-30-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must have the auditd service running.

```
GROUP ID: V-256490
RULE ID: SV-256490r958422
```

Rationale:

Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). They also provide a means to measure the impact of an event and help authorized personnel to determine the appropriate response.

Satisfies: 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-000445-GPOS-00199, SRG-OS-000446-GPOS-00200, SRG-OS-000461-GPOS-00205, SRG-OS-000467-GPOS-00211, SRG-OS-000465-GPOS-00209, SRG-OS-000474-GPOS-00219, SRG-OS-000475-GPOS-00220

Audit:

At the command line, run the following command:

```
# systemctl status auditd
```

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

Remediation:

At the command line, run the following commands:

```
# systemctl enable auditd
# systemctl start auditd
```

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-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-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-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-001814 The Information system supports auditing of the enforcement actions.

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

CCI-002696 Verify correct operation of organization-defined security functions.

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

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

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

1.14 PHTN-30-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system audit log must log space limit problems to syslog.

```
GROUP ID: V-256491
RULE ID: SV-256491r958424
```

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.

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

Audit:

At the command line, run the following command:

```
# grep "^space_left_action" /etc/audit/auditd.conf
```

Expected result:

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_action" line is uncommented and set to the following:

space_left_action = SYSLOG

At the command line, run the following commands:

```
# killproc auditd -TERM
# systemctl start 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)

1.15 PHTN-30-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system audit log must attempt to log audit failures to syslog.

```
GROUP ID: V-256492
RULE ID: SV-256492r1038966
```

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:

At the command line, run the following command:

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

If any of the above parameters 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 commands:

```
# killproc auditd -TERM
# systemctl start auditd
```

Additional Information:

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

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

1.16 PHTN-30-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system audit log must have correct permissions.

```
GROUP ID: V-256493
RULE ID: SV-256493r958434
```

Rationale:

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

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

Audit:

At the command line, run the following command:

```
# (audit_log_file=$(grep "^log_file" /etc/audit/auditd.conf|sed s/^[^\/]*//)
&& if [ -f "${audit_log_file}" ] ; then printf "Log(s) found in
"${audit_log_file%/*}":\n"; stat -c "%n permissions are %a"
${audit_log_file%}*; else printf "audit log file(s) not found\n"; fi)
```

If the permissions on any audit log file are more permissive than "0600", this is a finding.

Remediation:

At the command line, run the following command:

```
#  chmod 0600 <audit log file>
```

Replace `<audit log file>` with the log files more permissive than 0600.

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

1.17 PHTN-30-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system audit log must be owned by root.

```
GROUP ID: V-256494
RULE ID: SV-256494r958436
```

Rationale:

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

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

Audit:

At the command line, run the following command:

```
# (audit_log_file=$(grep "^log_file" /etc/audit/auditd.conf|sed s/^[^\/]*//)
&& if [ -f "${audit_log_file}" ] ; then printf "Log(s) found in
"${audit_log_file%/*}":\n"; stat -c "%n is owned by %U" ${audit_log_file%}*;
else printf "audit log file(s) not found\n"; fi)
```

If any audit log file is not owned by root, this is a finding.

Remediation:

At the command line, run the following command:

```
#  chown root:root <audit log file>
```

Replace `<audit log file>` with the log files not owned by root.

Additional Information:

CCI-000163 Protect audit information from unauthorized modification.

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

1.18 PHTN-30-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system audit log must be group-owned by root.

```
GROUP ID: V-256495
RULE ID: SV-256495r958438
```

Rationale:

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

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

Audit:

At the command line, run the following command:

```
# (audit_log_file=$(grep "^log_file" /etc/audit/auditd.conf|sed s/^[^\/]*//)
&& if [ -f "${audit_log_file}" ] ; then printf "Log(s) found in
"${audit_log_file%/*}":\n"; stat -c "%n is group owned by %G"
${audit_log_file%}*; else printf "audit log file(s) not found\n"; fi)
```

If any audit log file is not group owned by root, this is a finding.

Remediation:

At the command line, run the following command:

```
#  chown root:root <audit log file>
```

Replace `<audit log file>` with the log files not group owned by root.

Additional Information:

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

1.19 PHTN-30-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must allow only the information system security manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.

```
GROUP ID: V-256496
RULE ID: SV-256496r958444
```

Rationale:

Without the capability to restrict the roles and individuals that 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:

```
# find /etc/audit/* -type f -exec stat -c "%n permissions are %a" {} $1\;
```

If the permissions of any files are more permissive than "640", this is a finding.

Remediation:

At the command line, run the following command:

```
# chmod 640 <file>
```

Replace `<file>` with any file with incorrect permissions.

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

1.20 PHTN-30-000020 (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-256497
RULE ID: SV-256497r958446
```

Rationale:

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

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000468-GPOS-00212

Audit:

At the command line, run the following command:

```
# auditctl -l | grep chmod
```

Expected result:

```
-a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,fchownat,fchmodat -F
auid>=1000 -F auid!=4294967295 -F key=perm_mod

-a always,exit -F arch=b64 -S
chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lre
movexattr,fremovexattr,fchownat,fchmodat -F key=perm_mod

-a always,exit -F arch=b32 -S chmod,fchmod,fchown,chown,fchownat,fchmodat -F
auid>=1000 -F auid!=4294967295 -F key=perm_mod

-a always,exit -F arch=b32 -S
chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lre
movexattr,fremovexattr,fchownat,fchmodat -F key=perm_mod
```

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

Note: The auid!= parameter may display as 4294967295 or -1, which are equivalent.

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-30-000013.

Remediation:

Navigate to and open:

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

Add the following lines:

```
-a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,fchownat,fchmodat -F
auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b64 -S
chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lre
movexattr,fremovexattr,fchownat,fchmodat -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchown,chown,fchownat,fchmodat -F
auid>=1000 -F auid!=4294967295 -F key=perm_mod
-a always,exit -F arch=b32 -S
chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lre
movexattr,fremovexattr,fchownat,fchmodat -F key=perm_mod
```

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

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

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

1.21 PHTN-30-000021 (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-256498
RULE ID: SV-256498r982195
```

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.

Audit:

At the command line, run the following command:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always
"ucredit=.."
```

Expected result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include ucredit= <= -1, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-000192 The information system enforces password complexity by the minimum number of upper case characters used.

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

1.22 PHTN-30-000022 (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-256499
RULE ID: SV-256499r982196
```

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.

Audit:

At the command line, run the following command:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always
"lcredit=.."
```

Expected result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include lcredit= <= -1, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-000193 The information system enforces password complexity by the minimum number of lower case characters used.

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

1.23 PHTN-30-000023 (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-256500
RULE ID: SV-256500r982197
```

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.

Audit:

At the command line, run the following command:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always
"dcredit=.."
```

Expected result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include dcredit= <= -1, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-000194 The information system enforces password complexity by the minimum number of numeric characters used.

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

1.24 PHTN-30-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must require that new passwords are at least four characters different from the old password.

```
GROUP ID: V-256501
RULE ID: SV-256501r982198
```

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.

Audit:

At the command line, run the following command:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always "difok=."
```

Expected result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include difok >= 4, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

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

1.25 PHTN-30-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must store only encrypted representations of passwords.

```
GROUP ID: V-256502
RULE ID: SV-256502r982199
```

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:

```
# grep SHA512 /etc/login.defs|grep -v "#"
```

Expected result:

ENCRYPT_METHOD SHA512

If there is no output or if the output does match the expected result, this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Add or replace the ENCRYPT_METHOD line as follows:

ENCRYPT_METHOD SHA512

Additional Information:

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

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

1.26 PHTN-30-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must use an OpenSSH server version that does not support protocol 1.

```
GROUP ID: V-256503
RULE ID: SV-256503r987796
```

Rationale:

A replay attack may enable an unauthorized user to gain access to the operating system. Authentication sessions between the authenticator and the operating system validating the user credentials must not be vulnerable to a replay attack.

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.

A privileged account is any information system account with authorizations of a privileged user.

Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security). Additional techniques include time-synchronous or challenge-response one-time authenticators.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000395-GPOS-00175, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

At the command line, run the following command:

```
# rpm -qa|grep openssh
```

If there is no output or openssh is not >= version 7.4, this is a finding.

Remediation:

Installing openssh manually is not supported by VMware for appliances. Revert to a previous backup or redeploy the appliance.

Additional Information:

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

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

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

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

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

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

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

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

CCI-001942 The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (9)

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-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)

1.27 PHTN-30-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that passwords for new users are restricted to a 24-hour minimum lifetime.

```
GROUP ID: V-256504
RULE ID: SV-256504r982188
```

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, 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:

```
# grep "^PASS_MIN_DAYS" /etc/login.defs
```

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

Remediation:

Navigate to and open:

/etc/login.defs

Modify the "PASS_MIN_DAYS" line to the following:

PASS_MIN_DAYS 1

Additional Information:

CCI-000198 The information system enforces minimum password lifetime restrictions.

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

1.28 PHTN-30-000028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that passwords for new users are restricted to a 90-day maximum lifetime.

```
GROUP ID: V-256505
RULE ID: SV-256505r1038967
```

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:

```
# grep "^PASS_MAX_DAYS" /etc/login.defs
```

If the value of "PASS_MAX_DAYS" is greater than "90", this is a finding.

Remediation:

Navigate to and open:

/etc/login.def

Modify the "PASS_MAX_DAYS" line to the following:

PASS_MAX_DAYS 90

Additional Information:

CCI-000199 The information system enforces maximum password lifetime restrictions.

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

1.29 PHTN-30-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256506
RULE ID: SV-256506r982201
```

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 result is a password that is not changed per policy requirements.

Audit:

At the command line, run the following command:

```
# grep pam_pwhistory /etc/pam.d/system-password|grep --color=always
"remember=."
```

Expected result:

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

If the output does not include the "remember=5" setting as shown in the expected result, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following line after the "password requisite pam_cracklib.so" statement:

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

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-000200 The information system prohibits password reuse for the organization-defined number of generations.

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

1.30 PHTN-30-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256507
RULE ID: SV-256507r982202
```

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:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always
"minlen=.."
```

Example result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include minlen >= 8, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-000205 The information system enforces minimum password length.

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

1.31 PHTN-30-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-256508
RULE ID: SV-256508r958472
```

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:

```
# grep -i ^password_pbkdf2 /boot/grub2/grub.cfg
```

If there is not output, this is a finding.

If the output does not begin with "password_pbkdf2 root", this is a finding.

Remediation:

At the command line, run the following command:

```
# grub2-mkpasswd-pbkdf2
```

Enter a secure password and ensure this password is stored for break-glass situations. The vCenter root account cannot be recovered without knowing this separate password. Copy the resulting encrypted string.

An example string is below:

```
grub.pbkdf2.sha512.10000.983A13DF3C51BB2B5130F0B86DDBF0DEA1AAF766BD1F16B7840F
79CE3E35494C4B99F505C99C150071E563DF1D7FE1F45456D5960C4C79DAB6C49298B02A5558.
5B2C49E12D43CC5A876F6738462DE4EFC24939D4BE486CDB72CFBCD87FDE93FBAFCB817E01B90
F23E53C2502C3230502BC3113BE4F80B0AFC0EE956E735F7F86
```

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"
```

Below this, paste the following, substituting the encrypted string from the steps above:

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

Photon ships with one menuentry block by default. Copy that entire block and paste it right below itself.

Example:

```
menuentry "Photon" {
    linux "/"$photon_linux root=$rootpartition net.ifnames=0 $photon_cmdline
coredump_filter=0x37 consoleblank=0
    if [ "$photon_initrd" ]; then
        initrd "/"$photon_initrd
    fi
}
menuentry "Photon" {
    linux "/"$photon_linux root=$rootpartition net.ifnames=0 $photon_cmdline
coredump_filter=0x37 consoleblank=0
    if [ "$photon_initrd" ]; then
        initrd "/"$photon_initrd
    fi
}
```

Modify the first menuentry block to add the "--unrestricted" option as follows:

```
menuentry "Photon" --unrestricted {
```

Modify the second menuentry block to add the allowed user as follows:

```
menuentry "Recover Photon" --users root {
```

This concludes the fix. To verify, here is an example grub.cfg snippet:

```
...
set rootpartition=PARTUUID=326e5b0f-42fb-471a-8209-18964c4a2ed3
set superusers="root"
password_pbkdf2 root
grub.pbkdf2.sha512.10000.983A13DF3C51BB2B5130F0B86DDBF0DEA1AAF766BD1F16B7840F
79CE3E35494C4B99F505C99C150071E563DF1D7FE1F45456D5960C4C79DAB6C49298B02A5558.
5B2C49E12D43CC5A876F6738462DE4EFC24939D4BE486CDB72CFBCD87FDE93FBAFCB817E01B90
F23E53C2502C3230502BC3113BE4F80B0AFC0EE956E735F7F86

menuentry "Photon" --unrestricted {
    linux "/"$photon_linux root=$rootpartition net.ifnames=0 $photon_cmdline
coredump_filter=0x37 consoleblank=0
    if [ "$photon_initrd" ]; then
        initrd "/"$photon_initrd
    fi
}

menuentry "Recover Photon" --users root {
    linux "/"$photon_linux root=$rootpartition net.ifnames=0 $photon_cmdline
coredump_filter=0x37 consoleblank=0
    if [ "$photon_initrd" ]; then
        initrd "/"$photon_initrd
    fi
}
```

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

1.32 PHTN-30-000032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must disable the loading of unnecessary kernel modules.

```
GROUP ID: V-256509
RULE ID: SV-256509r958480
```

Rationale:

To support the requirements and principles of least functionality, the operating system must provide only essential capabilities and limit the use of modules, protocols, and/or services to only those required for the proper functioning of the product.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000114-GPOS-00059

Audit:

At the command line, run the following command:

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

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

CCI-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

1.33 PHTN-30-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256510
RULE ID: SV-256510r958482
```

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:

```
# 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

1.34 PHTN-30-000035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must disable new accounts immediately upon password expiration.

```
GROUP ID: V-256511
RULE ID: SV-256511r982189
```

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Disabling inactive accounts ensures accounts that may not have been responsibly removed are not available to attackers who may have compromised their credentials.

Audit:

At the command line, run the following command:

```
# grep INACTIVE /etc/default/useradd
```

Expected result:

INACTIVE=0

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

Remediation:

Navigate to and open:

/etc/default/useradd

Remove an existing "INACTIVE" line and add the following line:

INACTIVE=0

Additional Information:

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

1.35 PHTN-30-000036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must use Transmission Control Protocol (TCP) syncookies.

```
GROUP ID: V-256512
RULE ID: SV-256512r958528
```

Rationale:

A TCP SYN flood attack can cause a denial of service 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:

```
# /sbin/sysctl -a --pattern tcp_syncookies
```

Expected result:

net.ipv4.tcp_syncookies = 1

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

Remediation:

At the command line, run the following commands:

```
# sed -i -e "/^net.ipv4.tcp_syncookies/d" /etc/sysctl.conf
# echo net.ipv4.tcp_syncookies=1>>/etc/sysctl.conf
# /sbin/sysctl --load
```

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

1.36 PHTN-30-000037 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disconnect idle Secure Shell (SSH) sessions.

```
GROUP ID: V-256513
RULE ID: SV-256513r970703
```

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 a console or console port that has been left unattended.

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i ClientAliveInterval
```

Expected result:

ClientAliveInterval 900

If the output does not match the expected result, 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

1.37 PHTN-30-000038 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disconnect idle Secure Shell (SSH) sessions.

```
GROUP ID: V-256514
RULE ID: SV-256514r970703
```

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 a console or console port that has been left unattended.

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i ClientAliveCountMax
```

Expected result:

ClientAliveCountMax 0

If the output does not match the expected result, 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

1.38 PHTN-30-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system "/var/log" directory must be owned by root.

```
GROUP ID: V-256515
RULE ID: SV-256515r958566
```

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 and can provide sensitive information to an unprivileged attacker.

Audit:

At the command line, run the following command:

```
# stat -c "%n is owned by %U and group owned by %G" /var/log
```

If the "/var/log directory" is not owned by root, this is a finding.

Remediation:

At the command line, run the following command:

```
# chown root:root /var/log
```

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

1.39 PHTN-30-000041 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system messages file must have the correct ownership and file permissions.

```
GROUP ID: V-256516
RULE ID: SV-256516r958566
```

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 and can provide sensitive information to an unprivileged attacker.

Audit:

At the command line, run the following command:

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

If the "/var/log/messages" directory is not owned by root or not group owned by root, or the file permissions are more permission than "640", this is a finding.

Remediation:

At the command line, run the following commands:

```
# chown root:root /var/log/messages

# chmod 0640 /var/log/messages
```

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

1.40 PHTN-30-000042 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account modifications.

```
GROUP ID: V-256517
RULE ID: SV-256517r991551
```

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.

Audit:

At the command line, run the following command:

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

Expected result:

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

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-30-000013.

Remediation:

Navigate to and open:

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

Add 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: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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)

1.41 PHTN-30-000043 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account modifications.

```
GROUP ID: V-256518
RULE ID: SV-256518r991551
```

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.

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

Audit:

At the command line, run the following command:

```
# 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-30-000013.

Remediation:

Navigate to and open:

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

Add 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: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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)

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)

1.42 PHTN-30-000044 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account disabling actions.

```
GROUP ID: V-256519
RULE ID: SV-256519r991552
```

Rationale:

When operating system accounts are disabled, user accessibility is affected. Accounts are used for identifying individual users or operating system processes. To detect and respond to events affecting user accessibility and system processing, operating systems must audit account disabling actions.

Audit:

At the command line, run the following command:

```
 # auditctl -l | grep "w /usr/bin/passwd"
```

Expected result:

```
 -w /usr/bin/passwd -p x -k passwd
```

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-30-000013.

Remediation:

Navigate to and open:

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

Add the following lines:

```
-w /usr/bin/passwd -p x -k passwd
```

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

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

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

Additional Information:

CCI-001404 Automatically audit account disabling actions.

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

1.43 PHTN-30-000045 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit all account removal actions.

```
GROUP ID: V-256520
RULE ID: SV-256520r991553
```

Rationale:

When operating system accounts are removed, user accessibility is affected. Accounts are used for identifying individual users or operating system processes. To detect and respond to events affecting user accessibility and system processing, operating systems must audit account removal actions.

Audit:

At the command line, run the following command:

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

Expected result:

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

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. Enabling the auditd service is done in control PHTN-30-000013.

Remediation:

Navigate to and open:

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

Add 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: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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)

1.44 PHTN-30-000046 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must initiate auditing as part of the boot process.

```
GROUP ID: V-256521
RULE ID: SV-256521r991555
```

Rationale:

Each process on the system carries an "auditable" flag, which indicates whether its activities can be audited. Although auditd takes care of enabling this for all processes that launch after it starts, adding the kernel argument ensures the flag is set at boot for every process on the system. This includes processes created before auditd starts.

Audit:

At the command line, run the following command:

```
# grep "audit=1" /proc/cmdline
```

If no results are returned, this is a finding.

Remediation:

Navigate to and open:

/boot/grub2/grub.cfg

Locate the boot command line arguments. An example follows:

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

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

linux /$photon_linux root=$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)

1.45 PHTN-30-000047 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system audit files and directories must have correct permissions.

```
GROUP ID: V-256522
RULE ID: SV-256522r991557
```

Rationale:

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

Audit:

At the command line, run the following command:

```
# stat -c "%n is owned by %U and group owned by %G" /etc/audit/auditd.conf
```

If "auditd.conf" is not owned by root and group owned by root, this is a finding.

Remediation:

At the command line, run the following command:

```
# chown root:root /etc/audit/auditd.conf
```

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

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

1.46 PHTN-30-000048 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must protect audit tools from unauthorized modification and deletion.

```
GROUP ID: V-256523
RULE ID: SV-256523r991558
```

Rationale:

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

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

Audit:

At the command line, run the following command:

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

If any file is not owned by root or group-owned by root or permissions are more permissive than "750", this is a finding.

Remediation:

At the command line, run the following command for each file returned for user and group ownership:

```
# chown root:root <file>
```

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

```
# chmod 750 <file>
```

Additional Information:

CCI-001494 Protect audit tools from unauthorized modification.

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

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

1.47 PHTN-30-000050 (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-256524
RULE ID: SV-256524r991561
```

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.

Audit:

At the command line, run the following command:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always
"ocredit=.."
```

Expected result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include ocredit= <= -1, this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-001619 The information system enforces password complexity by the minimum number of special characters used.

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

1.48 PHTN-30-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system package files must not be modified.

```
GROUP ID: V-256525
RULE ID: SV-256525r991567
```

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.

Without confidence in the integrity of the auditing system and tools, the information it provides cannot be trusted.

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" | grep -v "^..........c"
```

If there is any output, this is a finding.

Remediation:

If the audit system binaries have been altered, the system must be taken offline and the information system security manager (ISSM) notified immediately.

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)

1.49 PHTN-30-000054 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256526
RULE ID: SV-256526r958732
```

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-000471-GPOS-00215

Audit:

At the command line, run the following command to obtain a list of setuid files:

```
# find / -xdev -path /var/lib/containerd -prune -o \( -perm -4000 -type f -o
-perm -2000 \) -type f -print | sort
```

Run the following command for each setuid file found in the first command:

```
# auditctl -l | grep <setuid_path>
```

Replace <setuid_path> with each path found in the first command.

If each <setuid_path> does not have a corresponding line in the audit rules, this is a finding.

A typical corresponding line will look like the following:

```
-a always,exit -S all -F path=<setuid_path> -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged
```

Note: The auid!= parameter may display as 4294967295 or -1, which are equivalent.

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-30-000013.

Remediation:

At the command line, run the following command to obtain a list of setuid files:

```
# find / -xdev -perm -4000 -type f -o -perm -2000 -type f | sort
```

Execute the following for each setuid file found in the first command 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=<setuid_path> -F perm=x -F auid>=1000 -F
auid!=4294967295 -F key=privileged
```

Execute the following command to load the new audit rules:

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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-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)

1.50 PHTN-30-000055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure auditd to keep five rotated log files.

```
GROUP ID: V-256527
RULE ID: SV-256527r958752
```

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 cron job, setting a reasonable number of logs to keep, and configuring auditd to not rotate the logs on its own. This ensures audit logs are accessible to the information system security officer (ISSO) in the event of a central log processing failure.

Audit:

At the command line, run the following command:

```
# grep "^num_logs" /etc/audit/auditd.conf
```

Expected result:

num_logs = 5

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

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Add or change the "num_logs" line as follows:

num_logs = 5

At the command line, run the following commands:

```
# killproc auditd -TERM
# systemctl start 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

1.51 PHTN-30-000056 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure auditd to keep logging in the event max log file size is reached.

```
GROUP ID: V-256528
RULE ID: SV-256528r958752
```

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 cron job, setting a reasonable number of logs to keep, and configuring auditd to not rotate the logs on its own. This ensures audit logs are accessible to the information system security officer (ISSO) in the event of a central log processing failure.

If another solution is not used to rotate auditd logs, auditd can be configured to rotate logs.

Audit:

At the command line, run the following command:

```
# grep "^max_log_file_action" /etc/audit/auditd.conf
```

Example result:

max_log_file_action = IGNORE

If logs are rotated outside of auditd with a tool such as logrotated, and this setting is not set to "IGNORE", this is a finding.

If logs are NOT rotated outside of auditd, and this setting is not set to "ROTATE", this is a finding.

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Add or change the "max_log_file_action" line as follows:

max_log_file_action = IGNORE

Note: This can also be set to "ROTATE" if another tool is not used to rotate auditd logs.

At the command line, run the following commands:

```
# killproc auditd -TERM
# systemctl start 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

1.52 PHTN-30-000057 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure auditd to log space limit problems to syslog.

```
GROUP ID: V-256529
RULE ID: SV-256529r971542
```

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:

```
# grep "^space_left " /etc/audit/auditd.conf
```

Expected result:

space_left = 75

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" line is uncommented and set to the following:

space_left = 75

At the command line, run the following commands:

```
# killproc auditd -TERM
# systemctl start 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)

1.53 PHTN-30-000059 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256530
RULE ID: SV-256530r982212
```

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. Ensuring all packages' cryptographic signatures are valid prior to installation ensures the provenance of the software and protects against malicious tampering.

Audit:

At the command line, run the following command:

```
# grep -s nosignature /usr/lib/rpm/rpmrc /etc/rpmrc ~root/.rpmrc
```

If the command returns any output, this is a finding.

Remediation:

Open the file containing "nosignature" with a text editor and remove the option.

Additional Information:

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

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

1.54 PHTN-30-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256531
RULE ID: SV-256531r982212
```

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. Cryptographically verifying the authenticity of all software packages during installation 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:

```
# grep "^gpgcheck" /etc/tdnf/tdnf.conf
```

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

Remediation:

Navigate to and open:

/etc/tdnf/tdnf.conf

Remove any existing "gpgcheck" setting and add the following line:

gpgcheck=1

Additional Information:

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

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

1.55 PHTN-30-000061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system YUM repository must cryptographically verify the authenticity of all software packages during installation.

```
GROUP ID: V-256532
RULE ID: SV-256532r982212
```

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. Cryptographically verifying the authenticity of all software packages during installation 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:

```
# 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.

Remove any existing "gpgcheck" setting and add the following line at the end of the file:

gpgcheck=1

Additional Information:

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

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

1.56 PHTN-30-000062 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256533
RULE ID: SV-256533r1050789
```

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:

```
# grep -ihs nopasswd /etc/sudoers /etc/sudoers.d/*|grep -v "^#"|grep -v
"^%"|awk '{print $1}'

# 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/<file name>
```

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

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

1.57 PHTN-30-000064 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Photon operating system must configure sshd to use FIPS 140-2 ciphers.

```
GROUP ID: V-256534
RULE ID: SV-256534r958850
```

Rationale:

Privileged access contains control and configuration information and is particularly sensitive, so additional protections are necessary. This is maintained by using cryptographic mechanisms such as encryption to protect confidentiality.

Nonlocal maintenance and diagnostic activities are conducted by individuals communicating through an external network (e.g., the internet) or internal network. Local maintenance and diagnostic activities are carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. It does not cover hardware/software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch).

The operating system can meet this requirement by leveraging a cryptographic module.

Satisfies: SRG-OS-000394-GPOS-00174, SRG-OS-000424-GPOS-00188

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i Ciphers
```

Expected result:

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

At the command line, run the following command:

```
# systemctl restart sshd.service
```

Additional Information:

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

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

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)

1.58 PHTN-30-000065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256535
RULE ID: SV-256535r958928
```

Rationale:

ASLR makes it more difficult for an attacker to predict the location of attack code they have introduced into a process's address space during an attempt at exploitation.

ASLR also makes it more difficult for an attacker to know the location of existing code to repurpose it using return-oriented programming (ROP) techniques.

Audit:

At the command line, run the following command:

```
# 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/50-security-hardening.conf

Ensure the "randomize_va_space" is uncommented and set to the following:

kernel.randomize_va_space=2

At the command line, run the following command:

```
# sysctl --system
```

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

1.59 PHTN-30-000066 (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-256536
RULE ID: SV-256536r958936
```

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
```

Expected result:

clean_requirements_on_remove=true

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

Remediation:

Navigate to and open:

/etc/tdnf/tdnf.conf

Remove any existing "clean_requirements_on_remove" line and ensure the following line is present:

clean_requirements_on_remove=true

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)

1.60 PHTN-30-000067 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must generate audit records when the sudo command is used.

```
GROUP ID: V-256537
RULE ID: SV-256537r991570
```

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-000458-GPOS-00203, SRG-OS-000463-GPOS-00207

Audit:

At the command line, run the following command:

```
# auditctl -l | grep sudo
```

Expected result:

```
-a always,exit -S all -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged
```

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

Note: The auid!= parameter may display as 4294967295 or -1, which are equivalent.

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-30-000013.

Remediation:

Navigate to and open:

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

Add the following line:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=4294967295 -F key=privileged
```

Execute the following command to load the new audit rules:

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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

1.61 PHTN-30-000068 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256538
RULE ID: SV-256538r991578
```

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-000470-GPOS-00214, SRG-OS-000472-GPOS-00217, SRG-OS-000473-GPOS-00218

Audit:

At the command line, run the following command:

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

Expected result:

```
-w /var/log/faillog -p wa
-w /var/log/lastlog -p wa
-w /var/log/tallylog -p wa
```

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-30-000013.

Remediation:

Navigate to and open:

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

Add the following lines:

```
-w /var/log/faillog -p wa
-w /var/log/lastlog -p wa
-w /var/log/tallylog -p wa
```

Execute the following command to load the new audit rules:

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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

1.62 PHTN-30-000069 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must audit the "insmod" module.

```
GROUP ID: V-256539
RULE ID: SV-256539r991580
```

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:

```
# auditctl -l | grep "/sbin/insmod"
```

Expected result:

```
-w /sbin/insmod -p x
```

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-30-000013.

Remediation:

Navigate to and open:

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

Add the following lines:

```
-w /sbin/insmod -p x
```

Execute the following command to load the new audit rules:

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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

1.63 PHTN-30-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system auditd service must generate audit records for all account creations, modifications, disabling, and termination events.

```
GROUP ID: V-256540
RULE ID: SV-256540r991585
```

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:

```
# auditctl -l | grep -E /etc/security/opasswd
```

If any of these are not listed with a permissions filter of at least "w", 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-30-000013.

Remediation:

Navigate to and open:

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

Add the following line:

```
-w /etc/security/opasswd -p wa -k opasswd
```

Execute the following command to load the new audit rules:

```
# /sbin/augenrules --load
```

Note: A new "audit.STIG.rules" file is provided for placement in "/etc/audit/rules.d" that contains all rules needed for auditd.

Note: An older "audit.STIG.rules" may exist if the file exists and references 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

1.64 PHTN-30-000071 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must use the "pam_cracklib" module.

```
GROUP ID: V-256541
RULE ID: SV-256541r991587
```

Rationale:

If the operating system allows the user to select passwords based on dictionary words, 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:

```
# grep pam_cracklib /etc/pam.d/system-password
```

If the output does not return at least "password requisite pam_cracklib.so", this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-000366 Implement the security configuration settings.

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

1.65 PHTN-30-000072 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must set the "FAIL_DELAY" parameter.

```
GROUP ID: V-256542
RULE ID: SV-256542r991588
```

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:

```
# grep FAIL_DELAY /etc/login.defs
```

Expected result:

FAIL_DELAY 4

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

Remediation:

Navigate to and open:

/etc/login.defs

Add the following line after the last auth statement:

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

1.66 PHTN-30-000073 (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-256543
RULE ID: SV-256543r991588
```

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:

```
# grep pam_faildelay /etc/pam.d/system-auth|grep --color=always "delay="
```

Expected result:

```
auth       optional pam_faildelay.so delay=4000000
```

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

Remediation:

Navigate to and open:

/etc/pam.d/system-auth

Remove any existing "pam_faildelay" line and add the following line at the end of the file:

```
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

1.67 PHTN-30-000074 (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-256544
RULE ID: SV-256544r991589
```

Rationale:

Without setting a balance between performance and ensuring all audit events are written to disk, performance of the system may suffer or the risk of missing audit entries may be too high.

Audit:

At the command line, run the following command:

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

Expected result:

flush = INCREMENTAL_ASYNC

freq = 50

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

Remediation:

Navigate to and open:

/etc/audit/auditd.conf

Ensure the following line is present and any existing "flush" and "freq" settings are removed:

```
flush = INCREMENTAL_ASYNC
freq = 50
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.68 PHTN-30-000075 (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-256545
RULE ID: SV-256545r991589
```

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:

```
# grep -i "^create_home" /etc/login.defs
```

If there is no output or the output does not equal "CREATE_HOME yes", this is a finding.

Remediation:

Navigate to and open:

/etc/login.defs

Ensure the following is present and any existing "CREATE_HOME" line is removed:

```
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

1.69 PHTN-30-000076 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256546
RULE ID: SV-256546r991589
```

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:

```
# systemctl status debug-shell.service|grep -E --color=always disabled
```

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

Remediation:

At the command line, run the following commands:

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

Reboot for changes to take effect.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.70 PHTN-30-000078 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256547
RULE ID: SV-256547r991589
```

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:

```
# sshd -T|&grep -i GSSAPIAuthentication
```

Expected result:

GSSAPIAuthentication no

If the output does not match the expected result, 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

1.71 PHTN-30-000079 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disable environment processing.

```
GROUP ID: V-256548
RULE ID: SV-256548r1051424
```

Rationale:

Enabling 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:

```
#sshd -T|&grep -i PermitUserEnvironment
```

Expected result:

PermitUserEnvironment no

If the output does not match the expected result, 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-30-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disable X11 forwarding.

```
GROUP ID: V-256549
RULE ID: SV-256549r991589
```

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:

```
# sshd -T|&grep -i X11Forwarding
```

Expected result:

X11Forwarding no

If the output does not match the expected result, 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

1.73 PHTN-30-000081 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to perform strict mode checking of home directory configuration files.

```
GROUP ID: V-256550
RULE ID: SV-256550r991589
```

Rationale:

If other users have access to modify user-specific Secure Shell (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:

```
# sshd -T|&grep -i StrictModes
```

Expected result:

StrictModes yes

If the output does not match the expected result, 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

1.74 PHTN-30-000082 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disallow Kerberos authentication.

```
GROUP ID: V-256551
RULE ID: SV-256551r991589
```

Rationale:

If Kerberos is enabled through Secure Shell (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:

```
# sshd -T|&grep -i KerberosAuthentication
```

Expected result:

KerberosAuthentication no

If the output does not match the expected result, 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

1.75 PHTN-30-000083 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disallow authentication with an empty password.

```
GROUP ID: V-256552
RULE ID: SV-256552r991589
```

Rationale:

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

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i PermitEmptyPasswords
```

Expected result:

PermitEmptyPasswords no

If the output does not match the expected result, 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

1.76 PHTN-30-000084 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disallow compression of the encrypted session stream.

```
GROUP ID: V-256553
RULE ID: SV-256553r991589
```

Rationale:

If compression is allowed in a Secure Shell (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:

```
# sshd -T|&grep -i Compression
```

Expected result:

Compression no

If the output does not match the expected result, 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

1.77 PHTN-30-000085 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to display the last login immediately after authentication.

```
GROUP ID: V-256554
RULE ID: SV-256554r991589
```

Rationale:

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

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i PrintLastLog
```

Expected result:

PrintLastLog yes

If the output does not match the expected result, 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

1.78 PHTN-30-000086 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to ignore user-specific trusted hosts lists.

```
GROUP ID: V-256555
RULE ID: SV-256555r991589
```

Rationale:

Secure Shell (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:

```
# sshd -T|&grep -i IgnoreRhosts
```

Expected result:

IgnoreRhosts yes

If the output does not match the expected result, 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

1.79 PHTN-30-000087 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to ignore user-specific "known_host" files.

```
GROUP ID: V-256556
RULE ID: SV-256556r991589
```

Rationale:

Secure Shell (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 that must also be ignored while disabling host-based authentication generally.

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i IgnoreUserKnownHosts
```

Expected result:

IgnoreUserKnownHosts yes

If the output does not match the expected result, 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

1.80 PHTN-30-000088 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to limit the number of allowed login attempts per connection.

```
GROUP ID: V-256557
RULE ID: SV-256557r991589
```

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:

```
# sshd -T|&grep -i MaxAuthTries
```

Expected result:

MaxAuthTries 6

If the output does not match the expected result, 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

1.81 PHTN-30-000089 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so the x86 Ctrl-Alt-Delete key sequence is disabled on the command line.

```
GROUP ID: V-256558
RULE ID: SV-256558r991589
```

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 operating system 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:

```
# systemctl status ctrl-alt-del.target
```

Expected result:

```
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 command:

```
# systemctl mask ctrl-alt-del.target
```

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-30-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so the "/etc/skel" default scripts are protected from unauthorized modification.

```
GROUP ID: V-256559
RULE ID: SV-256559r991589
```

Rationale:

If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files.

Audit:

At the command line, run the following command:

```
# stat -c "%n permissions are %a and owned by %U:%G" /etc/skel/.[^.]*
```

Expected result:

```
/etc/skel/.bash_logout permissions are 750 and owned by root:root
/etc/skel/.bash_profile permissions are 644 and owned by root:root
/etc/skel/.bashrc permissions are 750 and owned by root:root
```

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

Remediation:

At the command line, run the following commands:

```
# chmod 750 /etc/skel/.bash_logout
# chmod 644 /etc/skel/.bash_profile
# chmod 750 /etc/skel/.bashrc
# chown root:root /etc/skel/.bash_logout
# chown root:root /etc/skel/.bash_profile
# chown root:root /etc/skel/.bashrc
```

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-30-000091 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so the "/root" path is protected from unauthorized access.

```
GROUP ID: V-256560
RULE ID: SV-256560r991589
```

Rationale:

If the "/root" path is accessible to users other than root, unauthorized users could change the root partitions files.

Audit:

At the command line, run the following command:

```
# stat -c "%n permissions are %a and owned by %U:%G" /root
```

Expected result:

/root permissions are 700 and owned by root:root

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

Remediation:

At the command line, run the following commands:

```
# chmod 700 /root
# chown root:root /root
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.84 PHTN-30-000092 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that all global initialization scripts are protected from unauthorized modification.

```
GROUP ID: V-256561
RULE ID: SV-256561r991589
```

Rationale:

Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon login.

Audit:

At the command line, run the following command:

```
# find /etc/bash.bashrc /etc/profile /etc/profile.d/ -xdev -type f -a '(' -
perm -002 -o -not -user root -o -not -group root ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

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

```
# chmod o-w <file>
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.85 PHTN-30-000093 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that all system startup scripts are protected from unauthorized modification.

```
GROUP ID: V-256562
RULE ID: SV-256562r991589
```

Rationale:

If system startup scripts are accessible to unauthorized modification, this could compromise the system on startup.

Audit:

At the command line, run the following command:

```
# find /etc/rc.d/* -xdev -type f -a '(' -perm -002 -o -not -user root -o -not
-group root ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

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

```
# chmod o-w <file>
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.86 PHTN-30-000094 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that all files have a valid owner and group owner.

```
GROUP ID: V-256563
RULE ID: SV-256563r991589
```

Rationale:

If files do not have valid user and group owners, unintended access to files could occur.

Audit:

At the command line, run the following command:

```
# find / -fstype ext4 -nouser -o -nogroup -exec ls -ld {} \; 2>/dev/null
```

If any files are returned, this is a finding.

Remediation:

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

```
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.87 PHTN-30-000095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so the "/etc/cron.allow" file is protected from unauthorized modification.

```
GROUP ID: V-256564
RULE ID: SV-256564r991589
```

Rationale:

If cron files and folders are accessible to unauthorized users, malicious jobs may be created.

Audit:

At the command line, run the following command:

```
# stat -c "%n permissions are %a and owned by %U:%G" /etc/cron.allow
```

Expected result:

/etc/cron.allow permissions are 600 and owned by root:root

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

Remediation:

At the command line, run the following commands:

```
# chmod 600 /etc/cron.allow
# chown root:root /etc/cron.allow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.88 PHTN-30-000096 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that all cron jobs are protected from unauthorized modification.

```
GROUP ID: V-256565
RULE ID: SV-256565r991589
```

Rationale:

If cron files and folders are accessible to unauthorized users, malicious jobs may be created.

Audit:

At the command line, run the following command:

```
# find /etc/cron.d/ /etc/cron.daily/ /etc/cron.hourly/ /etc/cron.monthly/
/etc/cron.weekly/ -xdev -type f -a '(' -perm -022 -o -not -user root ')' -
exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

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

```
# chmod 644 <file>
# chown root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.89 PHTN-30-000097 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must be configured so that all cron paths are protected from unauthorized modification.

```
GROUP ID: V-256566
RULE ID: SV-256566r991589
```

Rationale:

If cron files and folders are accessible to unauthorized users, malicious jobs may be created.

Audit:

At the command line, run the following command:

```
# stat -c "%n permissions are %a and owned by %U:%G" /etc/cron.d
/etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly
```

Expected result:

```
/etc/cron.d permissions are 755 and owned by root:root
/etc/cron.daily permissions are 755 and owned by root:root
/etc/cron.hourly permissions are 755 and owned by root:root
/etc/cron.monthly permissions are 755 and owned by root:root
/etc/cron.weekly permissions are 755 and owned by root:root
```

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

Remediation:

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

```
# chmod 755 <path>
# chown root:root <path>
```

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-30-000098 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not forward IPv4 or IPv6 source-routed packets.

```
GROUP ID: V-256567
RULE ID: SV-256567r991589
```

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:

```
# /sbin/sysctl -a --pattern
"net.ipv[4|6].conf.(all|default|eth.*).accept_source_route"
```

Expected result:

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.eth0.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
net.ipv6.conf.eth0.accept_source_route = 0
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "0".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv[4|6].conf.(all|default|eth.*).accept_source_route"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=0>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000099 (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-256568
RULE ID: SV-256568r991589
```

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:

```
# /sbin/sysctl -a --pattern ignore_broadcasts
```

Expected result:

net.ipv4.icmp_echo_ignore_broadcasts = 1

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

Remediation:

At the command line, run the following commands:

```
# sed -i -e "/^net.ipv4.icmp_echo_ignore_broadcasts/d" /etc/sysctl.conf
# echo net.ipv4.icmp_echo_ignore_broadcasts=1>>/etc/sysctl.conf
# /sbin/sysctl --load
```

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-30-000100 (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-256569
RULE ID: SV-256569r991589
```

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:

```
# /sbin/sysctl -a --pattern
"net.ipv4.conf.(all|default|eth.*).accept_redirects"
```

Expected result:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "0".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv4.conf.(all|default|eth.*).accept_redirects"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=0>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000101 (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-256570
RULE ID: SV-256570r991589
```

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:

```
# /sbin/sysctl -a --pattern
"net.ipv4.conf.(all|default|eth.*).secure_redirects"
```

Expected result:

```
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.eth0.secure_redirects = 0
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "0".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv4.conf.(all|default|eth.*).secure_redirects"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=0>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000102 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not send IPv4 Internet Control Message Protocol (ICMP) redirects.

```
GROUP ID: V-256571
RULE ID: SV-256571r991589
```

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:

```
# /sbin/sysctl -a --pattern
"net.ipv4.conf.(all|default|eth.*).send_redirects"
```

Expected result:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.eth0.send_redirects = 0
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "0".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv4.conf.(all|default|eth.*).send_redirects"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=0>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000103 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must log IPv4 packets with impossible addresses.

```
GROUP ID: V-256572
RULE ID: SV-256572r991589
```

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:

```
# /sbin/sysctl -a --pattern "net.ipv4.conf.(all|default|eth.*).log_martians"
```

Expected result:

```
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.eth0.log_martians = 1
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "1".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv4.conf.(all|default|eth.*).log_martians"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=1>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000104 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must use a reverse-path filter for IPv4 network traffic.

```
GROUP ID: V-256573
RULE ID: SV-256573r991589
```

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:

```
# /sbin/sysctl -a --pattern "net.ipv4.conf.(all|default|eth.*)\.rp_filter"
```

Expected result:

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.eth0.rp_filter = 1
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "1".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv4.conf.(all|default|eth.*)\.rp_filter"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=1>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000105 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not perform multicast packet forwarding.

```
GROUP ID: V-256574
RULE ID: SV-256574r991589
```

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:

At the command line, run the following command:

```
# /sbin/sysctl -a --pattern
"net.ipv[4|6].conf.(all|default|eth.*).mc_forwarding"
```

Expected result:

```
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
```

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

Note: The number of "ethx" lines returned is dependent on the number of interfaces. Every "ethx" entry must be set to "0".

Remediation:

At the command line, run the following command:

```
# for SETTING in $(/sbin/sysctl -aN --pattern
"net.ipv[4|6].conf.(all|default|eth.*).mc_forwarding"); do sed -i -e
"/^${SETTING}/d" /etc/sysctl.conf;echo $SETTING=0>>/etc/sysctl.conf; done
# /sbin/sysctl --load
```

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-30-000106 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must not perform IPv4 packet forwarding.

```
GROUP ID: V-256575
RULE ID: SV-256575r991589
```

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:

At the command line, run the following command:

```
# /sbin/sysctl -a --pattern "net.ipv4.ip_forward$"
```

Expected result:

net.ipv4.ip_forward = 0

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

Remediation:

At the command line, run the following commands:

```
# sed -i -e "/^net.ipv4.ip_forward/d" /etc/sysctl.conf
# echo net.ipv4.ip_forward=0>>/etc/sysctl.conf
# /sbin/sysctl --load
```

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-30-000107 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must send Transmission Control Protocol (TCP) timestamps.

```
GROUP ID: V-256576
RULE ID: SV-256576r991589
```

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:

```
# /sbin/sysctl -a --pattern "net.ipv4.tcp_timestamps$"
```

Expected result:

net.ipv4.tcp_timestamps = 1

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

Remediation:

At the command line, run the following commands:

```
# sed -i -e "/^net.ipv4.tcp_timestamps/d" /etc/sysctl.conf
# echo net.ipv4.tcp_timestamps=1>>/etc/sysctl.conf
# /sbin/sysctl --load
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.100 PHTN-30-000108 (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-256577
RULE ID: SV-256577r991589
```

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
```

Expected result:

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

Remediation:

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

```
# chmod 644 <file>
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.101 PHTN-30-000109 (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-256578
RULE ID: SV-256578r991589
```

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
```

Expected 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 <file>
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.102 PHTN-30-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must enforce password complexity on the root account.

```
GROUP ID: V-256579
RULE ID: SV-256579r991589
```

Rationale:

Password complexity rules must apply to all accounts on the system, including root. Without specifying the "enforce_for_root flag", "pam_cracklib" 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:

```
# grep pam_cracklib /etc/pam.d/system-password|grep --color=always
"enforce_for_root"
```

Expected result:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_root

If the output does not include "enforce_for_root", this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the following, replacing any existing "pam_cracklib.so" line:

password requisite pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minlen=8 minclass=4 difok=4 retry=3 maxsequence=0 enforce_for_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-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-30-000111 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must protect all boot configuration files from unauthorized modification.

```
GROUP ID: V-256580
RULE ID: SV-256580r991589
```

Rationale:

Boot configuration files control how the system boots, including single-user mode, auditing, log levels, etc. Improper or malicious configurations can negatively affect system security and availability.

Audit:

At the command line, run the following command:

```
# find /boot/*.cfg -xdev -type f -a '(' -perm -002 -o -not -user root -o -not
-group root ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

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

```
# chmod 644 <file>
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.104 PHTN-30-000112 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must protect sshd configuration from unauthorized access.

```
GROUP ID: V-256581
RULE ID: SV-256581r991589
```

Rationale:

The "sshd_config" file contains all the configuration items for sshd. Incorrect or malicious configuration of sshd can allow unauthorized access to the system, insecure communication, limited forensic trail, etc.

Audit:

At the command line, run the following command:

```
# stat -c "%n permissions are %a and owned by %U:%G" /etc/ssh/sshd_config
```

Expected result:

/etc/ssh/sshd_config permissions are 600 and owned by root:root

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

Remediation:

At the command line, run the following commands:

```
# chmod 600 /etc/ssh/sshd_config
# chown root:root /etc/ssh/sshd_config
```

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-30-000113 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must protect all "sysctl" configuration files from unauthorized access.

```
GROUP ID: V-256582
RULE ID: SV-256582r991589
```

Rationale:

The "sysctl" configuration file specifies values for kernel parameters to be set on boot. Incorrect or malicious configuration of these parameters can have a negative effect on system security.

Audit:

At the command line, run the following command:

```
# find /etc/sysctl.conf /etc/sysctl.d/* -xdev -type f -a '(' -perm -002 -o -
not -user root -o -not -group root ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

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

```
# chmod 600 <file>
# chown root:root <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.106 PHTN-30-000114 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must set the "umask" parameter correctly.

```
GROUP ID: V-256583
RULE ID: SV-256583r991590
```

Rationale:

The "umask" value influences the permissions assigned to files when they are created. The "umask" setting in "login.defs" controls the permissions for a new user's home directory. By setting the proper "umask", home directories will only allow the new user to read and write files there.

Audit:

At the command line, run the following command:

```
# grep ^UMASK /etc/login.defs
```

Example result:

UMASK 077

If "UMASK" is not configured to "077", this a finding.

Note: "UMASK" should only be specified once in login.defs.

Remediation:

Navigate to and open:

/etc/login.defs

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

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

1.107 PHTN-30-000115 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to disallow HostbasedAuthentication.

```
GROUP ID: V-256584
RULE ID: SV-256584r991591
```

Rationale:

Secure Shell (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:

```
# sshd -T|&grep -i HostbasedAuthentication
```

Expected result:

hostbasedauthentication no

If the output does not match the expected result, 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

1.108 PHTN-30-000117 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must store only encrypted representations of passwords.

```
GROUP ID: V-256585
RULE ID: SV-256585r982199
```

Rationale:

Passwords must be protected at all times via strong, one-way encryption. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. If they are encrypted with a weak cipher, those passwords are much more vulnerable to offline brute-force attacks.

Audit:

At the command line, run the following command:

```
# grep password /etc/pam.d/system-password|grep --color=always "sha512"
```

If the output does not include "sha512", this is a finding.

Remediation:

Navigate to and open:

/etc/pam.d/system-password

Add the argument "sha512" to the "password" line:

password required pam_unix.so sha512 shadow try_first_pass

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

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

1.109 PHTN-30-000118 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must ensure the old passwords are being stored.

```
GROUP ID: V-256586
RULE ID: SV-256586r982201
```

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 result is a password that is not changed per policy requirements.

Audit:

At the command line, run the following command:

```
# ls -al /etc/security/opasswd
```

If "/etc/security/opasswd" does not exist, this is a finding.

Remediation:

At the command line, run the following commands:

```
# touch /etc/security/opasswd
# chown root:root /etc/security/opasswd
# chmod 0600 /etc/security/opasswd
```

Additional Information:

CCI-000200 The information system prohibits password reuse for the organization-defined number of generations.

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

1.110 PHTN-30-000119 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to restrict AllowTcpForwarding.

```
GROUP ID: V-256587
RULE ID: SV-256587r991589
```

Rationale:

While enabling Transmission Control Protocol (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:

```
# sshd -T|&grep -i AllowTcpForwarding
```

Expected result:

allowtcpforwarding no

If the output does not match the expected result, 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

1.111 PHTN-30-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must configure sshd to restrict LoginGraceTime.

```
GROUP ID: V-256588
RULE ID: SV-256588r991589
```

Rationale:

By default, sshd 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 resources and reduce the exposure any partial logon attempts may create.

Audit:

At the command line, run the following command:

```
# sshd -T|&grep -i LoginGraceTime
```

Expected result:

logingracetime 30

If the output does not match the expected result, 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

1.112 PHTN-30-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256589
RULE ID: SV-256589r959006
```

Rationale:

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

Audit:

At the command line, run the following command:

```
# cat /proc/sys/crypto/fips_enabled
```

If a value of "1" is not returned, this is a finding.

Remediation:

Navigate to and open:

/boot/grub2/grub.cfg

Locate the kernel command line, which will start with "linux", and add "fips=1" to the end. For example:

linux /$photon_linux audit=1 root=$rootpartition $photon_cmdline coredump_filter=0x37 consoleblank=0 $systemd_cmdline fips=1

Reboot the system for the change to take effect.

Note: The "fipsify" package must be installed for FIPS mode to work properly.

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

1.113 PHTN-30-000245 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Photon operating system must disable systemd fallback Domain Name System (DNS).

```
GROUP ID: V-256590
RULE ID: SV-256590r991589
```

Rationale:

Systemd contains an ability to set fallback DNS servers. This 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 information unknowingly in the event DNS is absent or misconfigured at the system level.

Audit:

At the command line, run the following command:

```
# 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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	PHTN-30-000001 (Manual)	☐	☐
1.2	PHTN-30-000002 (Manual)	☐	☐
1.3	PHTN-30-000003 (Manual)	☐	☐
1.4	PHTN-30-000004 (Manual)	☐	☐
1.5	PHTN-30-000005 (Manual)	☐	☐
1.6	PHTN-30-000006 (Manual)	☐	☐
1.7	PHTN-30-000007 (Manual)	☐	☐
1.8	PHTN-30-000008 (Manual)	☐	☐
1.9	PHTN-30-000009 (Manual)	☐	☐
1.10	PHTN-30-000010 (Manual)	☐	☐
1.11	PHTN-30-000011 (Manual)	☐	☐
1.12	PHTN-30-000012 (Manual)	☐	☐
1.13	PHTN-30-000013 (Manual)	☐	☐
1.14	PHTN-30-000014 (Manual)	☐	☐
1.15	PHTN-30-000015 (Manual)	☐	☐
1.16	PHTN-30-000016 (Manual)	☐	☐
1.17	PHTN-30-000017 (Manual)	☐	☐
1.18	PHTN-30-000018 (Manual)	☐	☐
1.19	PHTN-30-000019 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	PHTN-30-000020 (Manual)	☐	☐
1.21	PHTN-30-000021 (Manual)	☐	☐
1.22	PHTN-30-000022 (Manual)	☐	☐
1.23	PHTN-30-000023 (Manual)	☐	☐
1.24	PHTN-30-000024 (Manual)	☐	☐
1.25	PHTN-30-000025 (Manual)	☐	☐
1.26	PHTN-30-000026 (Manual)	☐	☐
1.27	PHTN-30-000027 (Manual)	☐	☐
1.28	PHTN-30-000028 (Manual)	☐	☐
1.29	PHTN-30-000029 (Manual)	☐	☐
1.30	PHTN-30-000030 (Manual)	☐	☐
1.31	PHTN-30-000031 (Manual)	☐	☐
1.32	PHTN-30-000032 (Manual)	☐	☐
1.33	PHTN-30-000033 (Manual)	☐	☐
1.34	PHTN-30-000035 (Manual)	☐	☐
1.35	PHTN-30-000036 (Manual)	☐	☐
1.36	PHTN-30-000037 (Manual)	☐	☐
1.37	PHTN-30-000038 (Manual)	☐	☐
1.38	PHTN-30-000040 (Manual)	☐	☐
1.39	PHTN-30-000041 (Manual)	☐	☐
1.40	PHTN-30-000042 (Manual)	☐	☐
1.41	PHTN-30-000043 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	PHTN-30-000044 (Manual)	☐	☐
1.43	PHTN-30-000045 (Manual)	☐	☐
1.44	PHTN-30-000046 (Manual)	☐	☐
1.45	PHTN-30-000047 (Manual)	☐	☐
1.46	PHTN-30-000048 (Manual)	☐	☐
1.47	PHTN-30-000050 (Manual)	☐	☐
1.48	PHTN-30-000051 (Manual)	☐	☐
1.49	PHTN-30-000054 (Manual)	☐	☐
1.50	PHTN-30-000055 (Manual)	☐	☐
1.51	PHTN-30-000056 (Manual)	☐	☐
1.52	PHTN-30-000057 (Manual)	☐	☐
1.53	PHTN-30-000059 (Manual)	☐	☐
1.54	PHTN-30-000060 (Manual)	☐	☐
1.55	PHTN-30-000061 (Manual)	☐	☐
1.56	PHTN-30-000062 (Manual)	☐	☐
1.57	PHTN-30-000064 (Manual)	☐	☐
1.58	PHTN-30-000065 (Manual)	☐	☐
1.59	PHTN-30-000066 (Manual)	☐	☐
1.60	PHTN-30-000067 (Manual)	☐	☐
1.61	PHTN-30-000068 (Manual)	☐	☐
1.62	PHTN-30-000069 (Manual)	☐	☐
1.63	PHTN-30-000070 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	PHTN-30-000071 (Manual)	☐	☐
1.65	PHTN-30-000072 (Manual)	☐	☐
1.66	PHTN-30-000073 (Manual)	☐	☐
1.67	PHTN-30-000074 (Manual)	☐	☐
1.68	PHTN-30-000075 (Manual)	☐	☐
1.69	PHTN-30-000076 (Manual)	☐	☐
1.70	PHTN-30-000078 (Manual)	☐	☐
1.71	PHTN-30-000079 (Manual)	☐	☐
1.72	PHTN-30-000080 (Manual)	☐	☐
1.73	PHTN-30-000081 (Manual)	☐	☐
1.74	PHTN-30-000082 (Manual)	☐	☐
1.75	PHTN-30-000083 (Manual)	☐	☐
1.76	PHTN-30-000084 (Manual)	☐	☐
1.77	PHTN-30-000085 (Manual)	☐	☐
1.78	PHTN-30-000086 (Manual)	☐	☐
1.79	PHTN-30-000087 (Manual)	☐	☐
1.80	PHTN-30-000088 (Manual)	☐	☐
1.81	PHTN-30-000089 (Manual)	☐	☐
1.82	PHTN-30-000090 (Manual)	☐	☐
1.83	PHTN-30-000091 (Manual)	☐	☐
1.84	PHTN-30-000092 (Manual)	☐	☐
1.85	PHTN-30-000093 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	PHTN-30-000094 (Manual)	☐	☐
1.87	PHTN-30-000095 (Manual)	☐	☐
1.88	PHTN-30-000096 (Manual)	☐	☐
1.89	PHTN-30-000097 (Manual)	☐	☐
1.90	PHTN-30-000098 (Manual)	☐	☐
1.91	PHTN-30-000099 (Manual)	☐	☐
1.92	PHTN-30-000100 (Manual)	☐	☐
1.93	PHTN-30-000101 (Manual)	☐	☐
1.94	PHTN-30-000102 (Manual)	☐	☐
1.95	PHTN-30-000103 (Manual)	☐	☐
1.96	PHTN-30-000104 (Manual)	☐	☐
1.97	PHTN-30-000105 (Manual)	☐	☐
1.98	PHTN-30-000106 (Manual)	☐	☐
1.99	PHTN-30-000107 (Manual)	☐	☐
1.100	PHTN-30-000108 (Manual)	☐	☐
1.101	PHTN-30-000109 (Manual)	☐	☐
1.102	PHTN-30-000110 (Manual)	☐	☐
1.103	PHTN-30-000111 (Manual)	☐	☐
1.104	PHTN-30-000112 (Manual)	☐	☐
1.105	PHTN-30-000113 (Manual)	☐	☐
1.106	PHTN-30-000114 (Manual)	☐	☐
1.107	PHTN-30-000115 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	PHTN-30-000117 (Manual)	☐	☐
1.109	PHTN-30-000118 (Manual)	☐	☐
1.110	PHTN-30-000119 (Manual)	☐	☐
1.111	PHTN-30-000120 (Manual)	☐	☐
1.112	PHTN-30-000240 (Manual)	☐	☐
1.113	PHTN-30-000245 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 20, 2025	1.0.0	Initial CIS Release