CIS VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) STIG Benchmark

v1.0.0 – 08-01-2024

Terms of Use

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

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

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

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

Table of Contents

Overview

Target Technology Details

VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) and are looking to comply with the STIG guidance

Recommendation Definitions

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.

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

The Rule Title from the STIG.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

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

Audit Procedure

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

Remediation Procedure

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

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

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

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

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI)

Recommendations

1 STIG RULES

VMware vSphere

VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

CLASSIFICATION unclassified

1.1 VCLD-80-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must limit the number of allowed simultaneous session requests.

```
GROUP ID: V-259137
RULE ID: SV-259137r1003685
```

Rationale:

Denial of service (DoS) is one threat against web servers. Many DoS attacks attempt to consume web server resources in such a way that no more resources are available to satisfy legitimate requests. Mitigation against these threats is to take steps to limit the number of resources that can be consumed in certain ways.

VAMI provides the "maxConnections" attribute of the <Connector Elements> to limit the number of concurrent Transmission Control Protocol (TCP) connections. This comes preconfigured with a tested, supported value that must be verified and maintained.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null |grep "server.max-connections"

Example result:

server.max-connections = 1024

If "server.max-connections" is not configured to 1024 or less, this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Add or reconfigure the following value:

server.max-connections = 1024

Restart the service with the following command:

systemctl restart cap-lighttpd

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

1.2 VCLD-80-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must use cryptography to protect the integrity of remote sessions.

```
GROUP ID: V-259138
RULE ID: SV-259138r1003688
```

Rationale:

Data exchanged between the user and the web server can range from static display data to credentials used to log in the hosted application. Even when data appears to be static, the nondisplayed logic in a web page may expose business logic or trusted system relationships. The integrity of all the data being exchanged between the user and web server must always be trusted. To protect the integrity and trust, encryption methods should be used to protect the complete communication session.

To protect the integrity and confidentiality of the remote sessions, VAMI uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

Satisfies: SRG-APP-000015-WSR-000014, SRG-APP-000315-WSR-000003

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "ssl.engine"

Example result:

ssl.engine = "enable"

If "ssl.engine" is not set to "enable", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

Add or reconfigure the following value:

ssl.engine = "enable"

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

CCI-002314 Employ automated mechanisms to control remote access methods.

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

1.3 VCLD-80-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must generate information to monitor remote access.

```
GROUP ID: V-259139
RULE ID: SV-259139r1003691
```

Rationale:

Remote access can be exploited by an attacker to compromise the server. By recording all remote access activities, it will be possible to determine the attacker's location, intent, and degree of success.

VAMI uses the "mod_accesslog" module to log information relating to remote requests. These logs can then be piped to external monitoring systems.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/server.modules/,/)/'|grep mod_accesslog

Example result:

"mod_accesslog",

If the "mod_accesslog" is not present, this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

Add the following value in the "server.modules" section:

mod_accesslog

The result should be similar to the following:

server.modules += ("mod_accesslog", "mod_cgi", "mod_magnet", "mod_rewrite")

Restart the service with the following command:

systemctl restart cap-lighttpd

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)

1.4 VCLD-80-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must produce log records containing sufficient information to establish what type of events occurred.

```
GROUP ID: V-259140
RULE ID: SV-259140r1003694
```

Rationale:

Web server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct type of event that occurred is important during forensic analysis. The correct determination of the event and when it occurred is important in relation to other events that happened at that same time.

Without sufficient information establishing what type of log event occurred, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, file names involved, access control, or flow control rules invoked.

Satisfies: SRG-APP-000095-WSR-000056, SRG-APP-000096-WSR-000057, SRG-APP-000097-WSR-000058, SRG-APP-000098-WSR-000059, SRG-APP-000099-WSR-000061, SRG-APP-000100-WSR-000064, SRG-APP-000374-WSR-000172, SRG-APP-000375-WSR-000171

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "accesslog.format"

The default commented, accesslog format is acceptable for this requirement. No output should be returned.

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

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Comment any existing accesslog.format lines by adding a "" at the beginning of the line.

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.5 VCLD-80-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service log files must only be accessible by privileged users.

```
GROUP ID: V-259141
RULE ID: SV-259141r960930
```

Rationale:

Log data is essential in the investigation of events. If log data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity would be difficult, if not impossible, to achieve. In addition, access to log records provides information an attacker could potentially use to their advantage since each event record might contain communication ports, protocols, services, trust relationships, user names, etc.

The web server must protect the log data from unauthorized read, write, copy, etc. This can be done by the web server if the web server is also doing the logging function. The web server may also use an external log system. In either case, the logs must be protected from access by nonprivileged users.

Satisfies: SRG-APP-000118-WSR-000068, SRG-APP-000119-WSR-000069, SRG-APP-000120-WSR-000070

Audit:

At the command prompt, run the following commands:

find /var/log/vmware/applmgmt/ /var/log/vmware/applmgmt-audit/ -xdev -type f -a '(' -perm -o+w -o -not -user root -o -not -group root ')' -exec ls -ld {} ;

find /opt/vmware/var/log/lighttpd/ -xdev -type f -a '(' -perm -o+w -o -not -user lighttpd -o -not -group lighttpd ')' -exec ls -ld {} ;

If any files are returned, this is a finding.

Remediation:

At the command prompt, run the following commands for log files under /opt/vmware/var/log/lighttpd/:

chmod o-w

chown lighttpd:lighttpd

At the command prompt, run the following commands for all other log files:

chmod o-w

chown root:root

Note: Substitute with the listed file.

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

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

CCI-000163 Protect audit information from unauthorized modification.

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

CCI-000164 Protect audit information from unauthorized deletion.

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

1.6 VCLD-80-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must off-load log records onto a different system or media from the system being logged.

```
GROUP ID: V-259142
RULE ID: SV-259142r960948
```

Rationale:

Protection of log data includes assuring log data is not accidentally lost or deleted. Backing up log records to an unrelated system or onto separate media than the system the web server is actually running on helps to assure that, in the event of a catastrophic system failure, the log records will be retained.

Satisfies: SRG-APP-000125-WSR-000071, SRG-APP-000358-WSR-000063, SRG-APP-000358-WSR-000163

Audit:

By default there is a vmware-services-applmgmt.conf rsyslog configuration file which includes the service logs when syslog is configured on vCenter that must be verified.

At the command prompt, run the following command:

cat /etc/vmware-syslog/vmware-services-applmgmt.conf

Expected result:

applmgmt.log

input(type="imfile"

File="/var/log/vmware/applmgmt/applmgmt.log"

Tag="applmgmt"

Severity="info"

Facility="local0")

applmgmt-audit.log

input(type="imfile"

File="/var/log/vmware/applmgmt-audit/applmgmt-audit.log"

Tag="applmgmt-audit"

Severity="info"
Facility="local0")
applmgmt-backup-restore-audit.log
input(type="imfile"
File="/var/log/vmware/applmgmt-audit/applmgmt-br-audit.log"
Tag="applmgmt-br-audit"
Severity="info"
Facility="local0")
vami-access.log
input(type="imfile"
File="/opt/vmware/var/log/lighttpd/access.log"
Tag="vami-access"
Severity="info"
Facility="local0")
vami-error.log
input(type="imfile"
File="/opt/vmware/var/log/lighttpd/error.log"
Tag="vami-error"
Severity="info"
Facility="local0")
dcui.log
input(type="imfile"
File="/var/log/vmware/applmgmt/dcui.log"
Tag="dcui"
Severity="info"
Facility="local0")
detwist.log
input(type="imfile"
File="/var/log/vmware/applmgmt/detwist.log"
Tag="detwist"

Severity="info"

Facility="local0")

firewall-reload.log

input(type="imfile"

File="/var/log/vmware/applmgmt/firewall-reload.log"

Tag="firewall-reload"

Severity="info"

Facility="local0")

applmgmt_vmonsvc.std*

input(type="imfile"

File="/var/log/vmware/applmgmt/applmgmt_vmonsvc.std*"

Tag="applmgmt_vmonsvc"

Severity="info"

Facility="local0")

backupSchedulerCron

input(type="imfile"

File="/var/log/vmware/applmgmt/backupSchedulerCron.log"

Tag="backupSchedulerCron"

Severity="info"

Facility="local0")

progress.log

input(type="imfile"

File="/var/log/vmware/applmgmt/progress.log"

Tag="progress"

Severity="info"

Facility="local0")

statsmoitor-alarms

input(type="imfile"

File="/var/log/vmware/statsmon/statsmoitor-alarms.log"

Tag="statsmoitor-alarms"

Severity="info"
Facility="local0")
StatsMonitor
input(type="imfile"
File="/var/log/vmware/statsmon/StatsMonitor.log"
Tag="StatsMonitor"
Severity="info"
Facility="local0")
StatsMonitorStartup.log.std*
input(type="imfile"
File="/var/log/vmware/statsmon/StatsMonitorStartup.log.std*"
Tag="StatsMonitor-Startup"
Severity="info"
Facility="local0")
PatchRunner
input(type="imfile"
File="/var/log/vmware/applmgmt/PatchRunner.log"
Tag="PatchRunner"
Severity="info"
Facility="local0")
update_microservice
input(type="imfile"
File="/var/log/vmware/applmgmt/update_microservice.log"
Tag="update_microservice"
Severity="info"
Facility="local0")
vami
input(type="imfile"
File="/var/log/vmware/applmgmt/vami.log"
Tag="vami"

Severity="info"
Facility="local0")
vcdb_pre_patch
input(type="imfile"
File="/var/log/vmware/applmgmt/vcdb_pre_patch.*"
Tag="vcdb_pre_patch"
Severity="info"
Facility="local0")
dnsmasq.log
input(type="imfile"
File="/var/log/vmware/dnsmasq.log"
Tag="dnsmasq"
Severity="info"
Facility="local0")
procstate
input(type="imfile"
File="/var/log/vmware/procstate"
Tag="procstate"
Severity="info"
Facility="local0")
backup.log
input(type="imfile"
File="/var/log/vmware/applmgmt/backup.log"
Tag="applmgmt-backup"
Severity="info"
Facility="local0")
size.log
input(type="imfile"
File="/var/log/vmware/applmgmt/size.log"
Tag="applmgmt-size"

Severity="info"

Facility="local0")

restore.log

input(type="imfile"

File="/var/log/vmware/applmgmt/restore.log"

Tag="applmgmt-restore"

Severity="info"

Facility="local0")

reconciliation.log

input(type="imfile"

File="/var/log/vmware/applmgmt/reconciliation.log"

Tag="applmgmt-reconciliation"

Severity="info"

Facility="local0")

pnid_change.log

input(type="imfile"

File="/var/log/vmware/applmgmt/pnid_change.log"

Tag="applmgmt-pnid-change"

Severity="info"

Facility="local0")

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

Remediation:

Navigate to and open:

/etc/vmware-syslog/vmware-services-applmgmt.conf

Create the file if it does not exist.

Set the contents of the file as follows:

applmgmt.log

input(type="imfile"

File="/var/log/vmware/applmgmt/applmgmt.log"

Tag="applmgmt"
Severity="info"
Facility="local0")
applmgmt-audit.log
input(type="imfile"
File="/var/log/vmware/applmgmt-audit/applmgmt-audit.log"
Tag="applmgmt-audit"
Severity="info"
Facility="local0")
applmgmt-backup-restore-audit.log
input(type="imfile"
File="/var/log/vmware/applmgmt-audit/applmgmt-br-audit.log"
Tag="applmgmt-br-audit"
Severity="info"
Facility="local0")
vami-access.log
input(type="imfile"
File="/opt/vmware/var/log/lighttpd/access.log"
Tag="vami-access"
Severity="info"
Facility="local0")
vami-error.log
input(type="imfile"
File="/opt/vmware/var/log/lighttpd/error.log"
Tag="vami-error"
Severity="info"
Facility="local0")
dcui.log
input(type="imfile"
File="/var/log/vmware/applmgmt/dcui.log"

Tag="dcui"
Severity="info"
Facility="local0")
detwist.log
input(type="imfile"
File="/var/log/vmware/applmgmt/detwist.log"
Tag="detwist"
Severity="info"
Facility="local0")
firewall-reload.log
input(type="imfile"
File="/var/log/vmware/applmgmt/firewall-reload.log"
Tag="firewall-reload"
Severity="info"
Facility="local0")
applmgmt_vmonsvc.std*
input(type="imfile"
File="/var/log/vmware/applmgmt/applmgmt_vmonsvc.std*"
Tag="applmgmt_vmonsvc"
Severity="info"
Facility="local0")
backupSchedulerCron
input(type="imfile"
File="/var/log/vmware/applmgmt/backupSchedulerCron.log"
Tag="backupSchedulerCron"
Severity="info"
Facility="local0")
progress.log
input(type="imfile"
File="/var/log/vmware/applmgmt/progress.log"

Tag="progress"
Severity="info"
Facility="local0")
statsmoitor-alarms
input(type="imfile"
File="/var/log/vmware/statsmon/statsmoitor-alarms.log"
Tag="statsmoitor-alarms"
Severity="info"
Facility="local0")
StatsMonitor
input(type="imfile"
File="/var/log/vmware/statsmon/StatsMonitor.log"
Tag="StatsMonitor"
Severity="info"
Facility="local0")
StatsMonitorStartup.log.std*
input(type="imfile"
File="/var/log/vmware/statsmon/StatsMonitorStartup.log.std*"
Tag="StatsMonitor-Startup"
Severity="info"
Facility="local0")
PatchRunner
input(type="imfile"
File="/var/log/vmware/applmgmt/PatchRunner.log"
Tag="PatchRunner"
Severity="info"
Facility="local0")
update_microservice
input(type="imfile"
File="/var/log/vmware/applmgmt/update_microservice.log"

Tag="update_microservice"
Severity="info"
Facility="local0")
vami
input(type="imfile"
File="/var/log/vmware/applmgmt/vami.log"
Tag="vami"
Severity="info"
Facility="local0")
vcdb_pre_patch
input(type="imfile"
File="/var/log/vmware/applmgmt/vcdb_pre_patch.*"
Tag="vcdb_pre_patch"
Severity="info"
Facility="local0")
dnsmasq.log
input(type="imfile"
File="/var/log/vmware/dnsmasq.log"
Tag="dnsmasq"
Severity="info"
Facility="local0")
procstate
input(type="imfile"
File="/var/log/vmware/procstate"
Tag="procstate"
Severity="info"
Facility="local0")
backup.log
input(type="imfile"
File="/var/log/vmware/applmgmt/backup.log"

Tag="applmgmt-backup"
Severity="info"
Facility="local0")
size.log
input(type="imfile"
File="/var/log/vmware/applmgmt/size.log"
Tag="applmgmt-size"
Severity="info"
Facility="local0")
restore.log
input(type="imfile"
File="/var/log/vmware/applmgmt/restore.log"
Tag="applmgmt-restore"
Severity="info"
Facility="local0")
reconciliation.log
input(type="imfile"
File="/var/log/vmware/applmgmt/reconciliation.log"
Tag="applmgmt-reconciliation"
Severity="info"
Facility="local0")
pnid_change.log
input(type="imfile"
File="/var/log/vmware/applmgmt/pnid_change.log"
Tag="applmgmt-pnid-change"
Severity="info"
Facility="local0")

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

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

1.7 VCLD-80-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must explicitly disable Multipurpose Internet Mail Extensions (MIME) mime mappings based on "Content-Type".

```
GROUP ID: V-259143
RULE ID: SV-259143r1003697
```

Rationale:

Controlling what a user of a hosted application can access is part of the security posture of the web server. Any time a user can access more functionality than is needed for the operation of the hosted application poses a security issue. A user with too much access can view information that is not needed for the user's job role, or the user could use the function in an unintentional manner.

A MIME tells the web server what type of program various file types and extensions are and what external utilities or programs are needed to execute the file type. A limited number of MIME types must be configured manually, and automatic mapping must be disabled.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "mimetype.use-xattr"

Example result:

mimetype.use-xattr="disable"

If "mimetype.use-xattr" is not set to "disable", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Add or reconfigure the following value:

mimetype.use-xattr = "disable"

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.8 VCLD-80-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must have resource mappings set to disable the serving of certain file types.

```
GROUP ID: V-259144
RULE ID: SV-259144r1003700
```

Rationale:

Resource mapping is the process of tying a particular file type to a process in the web server that can serve that type of file to a requesting client and to identify which file types are not to be delivered to a client.

By not specifying which files can and which files cannot be served to a user, VAMI could deliver sensitive files.

Audit:

At the command prompt, run the following command:

grep "url.access-deny" /var/lib/vmware/cap-lighttpd/lighttpd.conf

Example result:

url.access-deny = ("~", ".inc")

If "url.access-deny" is not set to "("~", ".inc")", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Add or reconfigure the following value:

url.access-deny = ("~", ".inc")

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.9 VCLD-80-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must have Web Distributed Authoring (WebDAV) disabled.

```
GROUP ID: V-259145
RULE ID: SV-259145r1003703
```

Rationale:

A web server can be installed with functionality that, by its nature, is not secure. WebDAV is an extension to the HTTP protocol that, when developed, was meant to allow users to create, change, and move documents on a server, typically a web server or web share. Allowing this functionality, development, and deployment is much easier for web authors.

WebDAV is not widely used and has serious security concerns because it may allow clients to modify unauthorized files on the web server.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/server.modules/,/)/'|grep mod_webdav

If any value is returned, this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Delete or comment out the "mod_webdav" line.

Note: The line may be in an included config and not in the parent config itself.

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.10 VCLD-80-000035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must protect system resources and privileged operations from hosted applications.

```
GROUP ID: V-259146
RULE ID: SV-259146r1003706
```

Rationale:

Most of the attention to denial-of-service (DoS) attacks focuses on ensuring that systems and applications are not victims of these attacks. However, these systems and applications must also be secured against use to launch such an attack against others.

A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks. Limiting system resources that are allocated to any user to a bare minimum may also reduce the ability of users to launch some DoS attacks.

One DoS mitigation is to prevent VAMI from keeping idle connections open for too long.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "server.max-keep-alive-idle"

Example result:

server.max-keep-alive-idle=30

If "server.max-keep-alive-idle" is not set to 30, this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf file.

Add or reconfigure the following value:

server.max-keep-alive-idle = 30

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.11 VCLD-80-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must restrict access to the web server's private key.

```
GROUP ID: V-259147
RULE ID: SV-259147r961041
```

Rationale:

The web server's private key is used to prove the identity of the server to clients and securely exchange the shared secret key used to encrypt communications between the web server and clients. By gaining access to the private key, an attacker can pretend to be an authorized server and decrypt the Secure Sockets Layer (SSL) traffic between a client and the web server.

Audit:

At the command prompt, run the following command:

stat -c "%n has %a permissions and is owned by %U:%G" /etc/applmgmt/appliance/server.pem

Expected result:

/etc/applmgmt/appliance/server.pem has 600 permissions and is owned by root:root

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

Remediation:

At the command prompt, run the following commands:

chown root:root /etc/applmgmt/appliance/server.pem

chmod 600 /etc/applmgmt/appliance/server.pem

Additional Information:

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

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

1.12 VCLD-80-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must restrict the ability of users to launch denial-of-service (DoS) attacks against other information systems or networks.

```
GROUP ID: V-259149
RULE ID: SV-259149r1003709
```

Rationale:

In UNIX and related computer operating systems, a file descriptor is an indicator used to access a file or other input/output resource, such as a pipe or network connection. File descriptors index into a per-process file descriptor table maintained by the kernel, which in turn indexes into a systemwide table of files opened by all processes, called the file table.

As a single-threaded server, Lighttpd must be limited in the number of file descriptors that can be allocated. This will prevent Lighttpd from being used in a form of DoS attack against the operating system.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "server.max-fds"

Example result:

server.max-fds=2048

If "server.max-fds" is not set to 2048 or less, this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Add or reconfigure the following value:

server.max-fds = 2048

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

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

1.13 VCLD-80-000061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must set the encoding for all text mime types to UTF-8.

```
GROUP ID: V-259150
RULE ID: SV-259150r1003712
```

Rationale:

Invalid user input occurs when a user inserts data or characters into a hosted application's data entry field and the hosted application is unprepared to process that data. This results in unanticipated application behavior, potentially leading to an application compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

An attacker can also enter Unicode into hosted applications in an effort to break out of the document home or root home directory or to bypass security checks.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/mimetype.assign/,/)/'|grep "text/"|grep -v "charset=utf-8"

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

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Navigate to the "mimetype.assign" block.

Replace all the mappings whose assigned type is "text/*" with mappings for UTF-8 encoding. For example:

".log" => "text/plain; charset=utf-8",

".conf" => "text/plain; charset=utf-8",

".text" => "text/plain; charset=utf-8",

".txt" => "text/plain; charset=utf-8",

".spec" => "text/plain; charset=utf-8",

".dtd" => "text/xml; charset=utf-8",

".xml" => "text/xml; charset=utf-8",

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

CCI-001310 Checks the validity of organization-defined information inputs to the system.

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

1.14 VCLD-80-000062 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must disable directory listing.

```
GROUP ID: V-259151
RULE ID: SV-259151r1003715
```

Rationale:

The goal is to completely control the web user's experience in navigating any portion of the web document root directories. Ensuring all web content directories have at least the equivalent of an "index.html" file is a significant factor to accomplish this end.

Enumeration techniques, such as Uniform Resource Locator (URL) parameter manipulation, rely on being able to obtain information about the web server's directory structure by locating directories without default pages. In this scenario, the web server will display to the user a listing of the files in the directory being accessed. By having a default hosted application web page, the anonymous web user will not obtain directory browsing information or an error message that reveals the server type and version.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "dir-listing.activate"

Example result:

dir-listing.activate = "disable"

If "dir-listing.activate" is not set to "disable", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Add or reconfigure the following value:

dir-listing.activate = "disable"

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.15 VCLD-80-000063 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must not be configured to use the "mod_status" module.

```
GROUP ID: V-259152
RULE ID: SV-259152r1003718
```

Rationale:

Any application providing too much information in error logs and in administrative messages to the screen risks compromising the data and security of the application and system.

VAMI must only generate error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages. The "mod_status" module generates the status overview of the webserver.

The information covers the following:

- Uptime.
- Average throughput.
- Current throughput.
- Active connections and their state.

While this information is useful on a development system, production systems must not have "mod_status" enabled.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/server.modules/,/)/'|grep mod_status

If any value is returned, this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf.

Remove the line containing "mod_status".

Note: The line may be in an included config and not in the parent config.

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.16 VCLD-80-000064 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must have debug logging disabled.

```
GROUP ID: V-259153
RULE ID: SV-259153r1003721
```

Rationale:

Information needed by an attacker to begin looking for possible vulnerabilities in a web server includes any information about the web server and plug-ins or modules being used. When debugging or trace information is enabled in a production web server, information about the web server, such as web server type, version, patches installed, plug-ins and modules installed, type of code being used by the hosted application, and any backends being used for data storage may be displayed.

Because this information may be placed in logs and general messages during normal operation of the web server, an attacker does not need to cause an error condition to gain this information.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "debug.log-request-handling"

Expected result:

debug.log-request-handling = "disable"

If "debug.log-request-handling" is not set to "disable", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Add or reconfigure the following value:

debug.log-request-handling = "disable"

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

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

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

1.17 VCLD-80-000097 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must disable client initiated TLS renegotiation.

```
GROUP ID: V-259155
RULE ID: SV-259155r1003724
```

Rationale:

All versions of the Secure Sockets Layer (SSL) and TLS protocols (up to and including TLS 1.2) are vulnerable to a man-in-the-middle attack (CVE-2009-3555) during a renegotiation. This vulnerability allows an attacker to "prefix" a chosen plaintext to the HTTP request as seen by the web server. The protocols have since been amended by RFC 5746, but the fix must be supported by both client and server to be effective.

While Lighttpd and the underlying OpenSSL libraries are no longer vulnerable, steps must be taken to account for older clients that do not support RFC 5746. To this end, Lighttpd disables client-initiated renegotiation entirely by default. This configuration must be validated and maintained.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "ssl.disable-client-renegotiation"

If no line is returned, this is not a finding.

If "ssl.disable-client-renegotiation" is set to "disabled", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/var/lib/vmware/cap-lighttpd/lighttpd.conf

Remove any setting for "ssl.disable-client-renegotiation".

Restart the service with the following command:

systemctl restart cap-lighttpd

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

1.18 VCLD-80-000098 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must be configured to hide the server type and version in client responses.

```
GROUP ID: V-259156
RULE ID: SV-259156r1003727
```

Rationale:

Web servers will often display error messages to client users, displaying enough information to aid in the debugging of the error. The information given back in error messages may display the web server type, version, patches installed, plug-ins and modules installed, type of code being used by the hosted application, and any backends being used for data storage.

This information could be used by an attacker to blueprint what type of attacks might be successful. Therefore, VAMI must be configured to hide the server version at all times.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|grep "server.tag"

Expected result:

server.tag = "vami"

If "server.tag" is not set to "vami", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

Add or reconfigure the following value:

server.tag = "vami"

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.19 VCLD-80-000099 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must implement HTTP Strict Transport Security (HSTS).

```
GROUP ID: V-259157
RULE ID: SV-259157r1003730
```

Rationale:

HSTS instructs web browsers to only use secure connections for all future requests when communicating with a website. Doing so helps prevent SSL protocol attacks, SSL stripping, cookie hijacking, and other attempts to circumvent SSL protection.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/setenv.add-response-header/,/)/'|sed -e 's/^[ ]*//'|grep "Strict-Transport-Security"

Example result:

```
"Strict-Transport-Security" => "max-age=31536000; includeSubDomains; preload"
```

If the response header "Strict-Transport-Security" is missing or not configured to "max-age=31536000; includeSubDomains; preload", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

If header "Strict-Transport-Security" is not present, add the following line to the end of the file:

setenv.add-response-header += ("Strict-Transport-Security" => "max-age=31536000; includeSubDomains; preload")

If header "Strict-Transport-Security" is present and not set to "Deny", update the value as shown below:

"Strict-Transport-Security" => "max-age=31536000; includeSubDomains; preload",

Note: The last line in the parameter does not need a trailing comma if part of a multi-line configuration.

Restart the service with the following command:

systemctl restart cap-lighttpd

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.20 VCLD-80-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must implement prevent rendering inside a frame or iframe on another site.

```
GROUP ID: V-259158
RULE ID: SV-259158r1003733
```

Rationale:

Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account but are instead typing into an invisible frame controlled by the attacker.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/setenv.add-response-header/,/)/'|sed -e 's/^[ ]*//'|grep "X-Frame-Options"

Example result:

"X-Frame-Options" => "Deny",

If the response header "X-Frame-Options" is missing or not configured to "Deny", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

If header "X-Frame-Options" is not present, add the following line to the end of the file:

setenv.add-response-header += ("X-Frame-Options" => "Deny")

If header "X-Frame-Options" is present and not set to "Deny", update the value as shown below:

"X-Frame-Options" => "Deny",

Note: The last line in the parameter does not need a trailing comma if part of a multi-line configuration.

Restart the service with the following command:

systemctl restart cap-lighttpd

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

1.21 VCLD-80-000101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must protect against MIME sniffing.

```
GROUP ID: V-259159
RULE ID: SV-259159r1003736
```

Rationale:

MIME sniffing was, and still is, a technique used by some web browsers to examine the content of a particular asset. This is done for the purpose of determining an asset's file format. This technique is useful in the event that there is not enough metadata information present for a particular asset, thus leaving the possibility that the browser interprets the asset incorrectly.

Although MIME sniffing can be useful to determine an asset's correct file format, it can also cause a security vulnerability. This vulnerability can be quite dangerous both for site owners as well as site visitors. This is because an attacker can leverage MIME sniffing to send an XSS (Cross Site Scripting) attack.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/setenv.add-response-header/,/)/'|sed -e 's/^[ ]*//'|grep "X-Content-Type-Options"

Example result:

"X-Content-Type-Options" => "nosniff",

If the response header "X-Content-Type-Options" is missing or not configured to "nosniff", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

If header "X-Content-Type-Options" is not present, add the following line to the end of the file:

setenv.add-response-header += ("X-Content-Type-Options" => "nosniff")

If header "X-Content-Type-Options" is present and not set to "nosniff", update the value as shown below:

"X-Content-Type-Options" => "nosniff",

Note: The last line in the parameter does not need a trailing comma if part of a multi-line configuration.

Restart the service with the following command:

systemctl restart cap-lighttpd

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

1.22 VCLD-80-000102 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter VAMI service must enable Content Security Policy.

```
GROUP ID: V-259160
RULE ID: SV-259160r1003739
```

Rationale:

A Content Security Policy (CSP) requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browsers render pages (e.g., inline JavaScript is disabled by default and must be explicitly allowed in the policy). CSP prevents a wide range of attacks, including cross-site scripting and other cross-site injections.

Audit:

At the command prompt, run the following command:

/opt/vmware/cap_lighttpd/sbin/lighttpd -p -f /var/lib/vmware/cap-lighttpd/lighttpd.conf 2>/dev/null|awk '/setenv.add-response-header/,/)/'|sed -e 's/^[ ]*//'|grep "Content-Security-Policy"

Example result:

```
"Content-Security-Policy" => "default-src 'self'; img-src 'self' data:
https://vcsa.vmware.com; font-src 'self' data:; object-src 'none'; style-src
'self' 'unsafe-inline'"
```

If the response header "Content-Security-Policy" is missing or not configured to "default-src 'self'; img-src 'self' data: https://vcsa.vmware.com; font-src 'self' data:; object-src 'none'; style-src 'self' 'unsafe-inline'", this is a finding.

Note: The command must be run from a bash shell and not from a shell generated by the "appliance shell". Use the "chsh" command to change the shell for the account to "/bin/bash". Refer to KB Article 2100508 for more details:

https://kb.vmware.com/s/article/2100508

Remediation:

Navigate to and open:

/opt/vmware/etc/lighttpd/applmgmt-lighttpd.conf

If header "Content-Security-Policy" is not present, add the following line to the end of the file:

setenv.add-response-header += ("Content-Security-Policy" => "default-src 'self'; img-src 'self' data: https://vcsa.vmware.com; font-src 'self' data:; object-src 'none'; style-src 'self' 'unsafe-inline'")

If header "Content-Security-Policy" is present and not set to "default-src 'self'; img-src 'self' data: https://vcsa.vmware.com; font-src 'self' data:; object-src 'none'; style-src 'self' 'unsafe-inline'", update the value as shown below:

"Content-Security-Policy" => "default-src 'self'; img-src 'self' data: https://vcsa.vmware.com; font-src 'self' data:; object-src 'none'; style-src 'self' 'unsafe-inline'",

Note: The last line in the parameter does not need a trailing comma if part of a multi-line configuration.

Restart the service with the following command:

systemctl restart cap-lighttpd

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	VCLD-80-000001 (Manual)	☐	☐
1.2	VCLD-80-000004 (Manual)	☐	☐
1.3	VCLD-80-000005 (Manual)	☐	☐
1.4	VCLD-80-000010 (Manual)	☐	☐
1.5	VCLD-80-000019 (Manual)	☐	☐
1.6	VCLD-80-000022 (Manual)	☐	☐
1.7	VCLD-80-000031 (Manual)	☐	☐
1.8	VCLD-80-000033 (Manual)	☐	☐
1.9	VCLD-80-000034 (Manual)	☐	☐
1.10	VCLD-80-000035 (Manual)	☐	☐
1.11	VCLD-80-000040 (Manual)	☐	☐
1.12	VCLD-80-000060 (Manual)	☐	☐
1.13	VCLD-80-000061 (Manual)	☐	☐
1.14	VCLD-80-000062 (Manual)	☐	☐
1.15	VCLD-80-000063 (Manual)	☐	☐
1.16	VCLD-80-000064 (Manual)	☐	☐
1.17	VCLD-80-000097 (Manual)	☐	☐
1.18	VCLD-80-000098 (Manual)	☐	☐
1.19	VCLD-80-000099 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	VCLD-80-000100 (Manual)	☐	☐
1.21	VCLD-80-000101 (Manual)	☐	☐
1.22	VCLD-80-000102 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
09-09-2025	1.0.0	Initial CIS Release