CIS VMware vSphere 8.0 vCenter Appliance Envoy STIG Benchmark

v1.0.0 – 08-01-2025

Terms of Use

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

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

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

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

Table of Contents

Overview

Target Technology Details

VMware vSphere 8.0 vCenter Appliance Envoy 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 Envoy 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

Supplementary information that does not correspond to any other field but may be useful to the user.

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 Envoy

Recommendations

1 STIG RULES

VMware vSphere

VMware vSphere 8.0 vCenter Appliance Envoy Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

CLASSIFICATION unclassified

1.1 VCRP-80-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Envoy and Rhttpproxy service log files permissions must be set correctly.

```
GROUP ID: V-259161
RULE ID: SV-259161r960930
```

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, usernames, 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/rhttpproxy/ -xdev -type f -a '(' -perm -o+w -o -not -user rhttpproxy -o -not -group rhttpproxy ')' -exec ls -ld {} ;

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

If any files are returned, this is a finding.

Remediation:

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

chmod o-w

chown rhttpproxy:rhttpproxy

or

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

chmod o-w

chown envoy:envoy

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

1.2 VCRP-80-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Envoy service private key file must be protected from unauthorized access.

```
GROUP ID: V-259162
RULE ID: SV-259162r961041
```

Rationale:

Envoy'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 Transport Layer Security (TLS) traffic between a client and the web server.

Audit:

At the command prompt, run the following command:

stat -c "%n permissions are %a, is owned by %U and group owned by %G" /etc/vmware-rhttpproxy/ssl/rui.key

Expected result:

/etc/vmware-rhttpproxy/ssl/rui.key permissions are 600, is owned by rhttpproxy and group owned by rhttpproxy

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

Remediation:

At the command prompt, run the following commands:

chmod 600 /etc/vmware-rhttpproxy/ssl/rui.key

chown rhttpproxy:rhttpproxy /etc/vmware-rhttpproxy/ssl/rui.key

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)

1.3 VCRP-80-000073 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Rhttpproxy service log files must be sent to a central log server.

```
GROUP ID: V-259163
RULE ID: SV-259163r961395
```

Rationale:

Writing events to a centralized management audit system offers many benefits to the enterprise over having dispersed logs. Centralized management of audit records and logs provides for efficiency in maintenance and management of records, enterprise analysis of events, and backup and archiving of event records enterprise-wide. The web server and related components are required to be capable of writing logs to centralized audit log servers.

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

Audit:

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

At the command prompt, run the following command:

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

Expected result:

rhttpproxy log

input(type="imfile"

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

Tag="rhttpproxy-main"

Severity="info"

Facility="local0")

rhttpproxy init stdout

input(type="imfile"

File="/var/log/vmware/rhttpproxy/rproxy_init.log.stdout"

Tag="rhttpproxy-stdout"

Severity="info"

Facility="local0")

rhttpproxy init stderr

input(type="imfile"

File="/var/log/vmware/rhttpproxy/rproxy_init.log.stderr"

Tag="rhttpproxy-stderr"

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-rhttpproxy.conf

Create the file if it does not exist.

Set the contents of the file as follows:

rhttpproxy log

input(type="imfile"

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

Tag="rhttpproxy-main"

Severity="info"

Facility="local0")

rhttpproxy init stdout

input(type="imfile"

File="/var/log/vmware/rhttpproxy/rproxy_init.log.stdout"

Tag="rhttpproxy-stdout"

Severity="info"

Facility="local0")

rhttpproxy init stderr

input(type="imfile"

File="/var/log/vmware/rhttpproxy/rproxy_init.log.stderr"

Tag="rhttpproxy-stderr"

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)

1.4 VCRP-80-000097 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Envoy service log files must be sent to a central log server.

```
GROUP ID: V-259164
RULE ID: SV-259164r961395
```

Rationale:

Writing events to a centralized management audit system offers many benefits to the enterprise over having dispersed logs. Centralized management of audit records and logs provides for efficiency in maintenance and management of records, enterprise analysis of events, and backup and archiving of event records enterprise-wide. The web server and related components are required to be capable of writing logs to centralized audit log servers.

Audit:

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

At the command prompt, run the following command:

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

Expected result:

envoy service log

input(type="imfile"

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

Tag="envoy-main"

Severity="info"

Facility="local0")

envoy access log

input(type="imfile"

File="/var/log/vmware/envoy/envoy-access.log"

Tag="envoy-access"

Severity="info"

Facility="local0")

envoy init stdout

input(type="imfile"

File="/var/log/vmware/envoy/envoy_init.log.stdout"

Tag="envoy-stdout"

Severity="info"

Facility="local0")

envoy init stderr

input(type="imfile"

File="/var/log/vmware/envoy/envoy_init.log.stderr"

Tag="envoy-stderr"

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-envoy.conf

Create the file if it does not exist.

Set the contents of the file as follows:

envoy service log

input(type="imfile"

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

Tag="envoy-main"

Severity="info"

Facility="local0")

envoy access log

input(type="imfile"

File="/var/log/vmware/envoy/envoy-access.log"

Tag="envoy-access"

Severity="info"

Facility="local0")

envoy init stdout

input(type="imfile"

File="/var/log/vmware/envoy/envoy_init.log.stdout"

Tag="envoy-stdout"

Severity="info"

Facility="local0")

envoy init stderr

input(type="imfile"

File="/var/log/vmware/envoy/envoy_init.log.stderr"

Tag="envoy-stderr"

Severity="info"

Facility="local0")

Additional Information:

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)

1.5 VCRP-80-000098 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Envoy service must set a limit on remote connections.

```
GROUP ID: V-259165
RULE ID: SV-259165r960735
```

Rationale:

Envoy client connections must be limited to preserve system resources and continue servicing connections without interruption. Without a limit set, the system would be vulnerable to a trivial denial-of-service attack where connections are created en masse and vCenter resources are entirely consumed.

Envoy comes hard coded with a tested and supported value for "maxRemoteHttpsConnections" and "maxRemoteHttpConnections" that must be verified and maintained.

Audit:

At the command prompt, run the following commands:

xmllint --xpath '/config/envoy/L4Filter/maxRemoteHttpsConnections/text()' /etc/vmware-rhttpproxy/config.xml

xmllint --xpath '/config/envoy/L4Filter/maxRemoteHttpConnections/text()' /etc/vmware-rhttpproxy/config.xml

Example result:

2048

or

XPath set is empty

If the output is not "2048" or "XPath set it empty", this is a finding.

Note: If "XPath set is empty" is returned the default values are in effect and is 2048.

Remediation:

Navigate to and open:

/etc/vmware-rhttpproxy/config.xml

Locate the //<L4Filter> block and configure it as follows:

<maxRemoteHttpsConnections>2048</maxRemoteHttpsConnections>

<maxRemoteHttpConnections>2048</maxRemoteHttpConnections>

Restart the service for changes to take effect.

vmon-cli --restart rhttpproxy

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCRP-80-000019 (Manual)	☐	☐
1.2	VCRP-80-000040 (Manual)	☐	☐
1.3	VCRP-80-000073 (Manual)	☐	☐
1.4	VCRP-80-000097 (Manual)	☐	☐
1.5	VCRP-80-000098 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
09-08-2025	1.0.0	Initial CIS Release