CIS VMware vSphere 7.0 vCenter Appliance RhttpProxy 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

Overview

Target Technology Details

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

Version: 1 Release: 1 Benchmark

Date: 07 Mar 2023

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 RhttpProxy 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 RhttpProxy

Recommendations

1 STIG RULES

VMware vSphere 7.0

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

Version: 1 Release: 1 Benchmark

Date: 07 Mar 2023

CLASSIFICATION unclassified

1.1 VCRP-70-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy must drop connections to disconnected clients.

```
GROUP ID: V-256737
RULE ID: SV-256737r889149
```

Rationale:

Envoy client connections that are established but no longer connected can consume resources that might otherwise be required by active connections. It is a best practice to terminate connections that are no longer connected to an active client.

Envoy is hard coded to drop connections after three minutes of idle time. The absence of any "tcpKeepAliveTimeSec" settings means this default is in effect. This configuration must be verified and maintained.

Audit:

At the command prompt, run the following command:

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

Expected result:

180

or

XPath set is empty

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

Remediation:

Navigate to and open:

/etc/vmware-rhttpproxy/config.xml

Locate the <config>/<envoy>/<L4Filter> block and configure <tcpKeepAliveTimeSec> as follows:

```
<tcpKeepAliveTimeSec>180</tcpKeepAliveTimeSec>
```

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

1.2 VCRP-70-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy must set a limit on established connections.

```
GROUP ID: V-256738
RULE ID: SV-256738r889152
```

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 "maxHttpsConnections" that must be verified and maintained.

Audit:

At the command prompt, run the following command:

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

Expected result:

2048

or

XPath set is empty

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

Remediation:

Navigate to and open:

/etc/vmware-rhttpproxy/config.xml

Locate the <config>/<envoy>/<L4Filter> block and configure <maxHttpsConnections> as follows:

```
<maxHttpsConnections>2048</maxHttpsConnections>
```

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

1.3 VCRP-70-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy must be configured to operate in FIPS mode.

```
GROUP ID: V-256739
RULE ID: SV-256739r889155
```

Rationale:

Envoy ships with FIPS 140-2 validated OpenSSL cryptographic libraries and is configured by default to run in FIPS mode. This module is used for all cryptographic operations performed by Envoy, including protection of data-in-transit over the client Transport Layer Security (TLS) connection.

Satisfies: SRG-APP-000014-WSR-000006, SRG-APP-000179-WSR-000111, SRG-APP-000416-WSR-000118, SRG-APP-000439-WSR-000188, SRG-APP-000179-WSR-000110

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath '/config/vmacore/ssl/fips' /etc/vmware-
rhttpproxy/config.xml
```

Expected result:

```
<fips>true</fips>
```

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

Remediation:

Navigate to and open:

/etc/vmware-rhttpproxy/config.xml

Locate the `<config>/<vmacore>/<ssl>` block and configure `<fips>` as follows:

```
<fips>true</fips>
```

Restart the service for changes to take effect.

```
# vmon-cli --restart rhttpproxy
```

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-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-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

1.4 VCRP-70-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy must use only Transport Layer Security (TLS) 1.2 for the protection of client connections.

```
GROUP ID: V-256740
RULE ID: SV-256740r889158
```

Rationale:

Envoy can be configured to support TLS 1.0, 1.1, and 1.2. Due to intrinsic problems in TLS 1.0 and TLS 1.1, they are disabled by default. The block in the rhttpproxy configuration is commented out by default, and this configuration forces TLS 1.2.

The block may also be set to "tls1.2" in certain upgrade scenarios, but the effect is the same. Uncommenting the block and enabling older protocols is possible; therefore, TLS 1.2 restriction must be verified and maintained.

Satisfies: SRG-APP-000015-WSR-000014, SRG-APP-000172-WSR-000104, SRG-APP-000439-WSR-000151, SRG-APP-000439-WSR-000152, SRG-APP-000439-WSR-000156, SRG-APP-000441-WSR-000181, SRG-APP-000442-WSR-000182

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath '/config/vmacore/ssl/protocols' /etc/vmware-
rhttpproxy/config.xml
```

Expected result:

XPath set is empty

or

```
<protocols>tls1.2</protocols>
```

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

Remediation:

Navigate to and open:

/etc/vmware-rhttpproxy/config.xml

Locate the `<config>/<vmacore>/<ssl>` block and configure `<protocols>` as follows:

```
<protocols>tls1.2</protocols>
```

Restart the service for changes to take effect.

```
# vmon-cli --restart rhttpproxy
```

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-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-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)

1.5 VCRP-70-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256741
RULE ID: SV-256741r889161
```

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 root and group owned by root

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 root:root /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)

1.6 VCRP-70-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy must exclusively use the HTTPS protocol for client connections.

```
GROUP ID: V-256742
RULE ID: SV-256742r889164
```

Rationale:

Remotely accessing vCenter via Envoy involves sensitive information going over the wire. To protect the confidentiality and integrity of these communications, Envoy must be configured to use an encrypted session of HTTPS rather than plain-text HTTP. The Secure Sockets Layer (SSL) configuration block inside the rhttpproxy configuration must be present and correctly configured to safely enable Transport Layer Security (TLS).

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath '/config/ssl' /etc/vmware-rhttpproxy/config.xml
```

Expected result:

```
<ssl>
    <!-- The server private key file -->
    <privateKey>/etc/vmware-rhttpproxy/ssl/rui.key</privateKey>
    <!-- The server side certificate file -->
    <certificate>/etc/vmware-rhttpproxy/ssl/rui.crt</certificate>
    <!-- vecs server name. Currently vecs runs on all node types. -->
    <vecsServerName>localhost</vecsServerName>
  </ssl>
```

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

Remediation:

Navigate to and open:

/etc/vmware-rhttpproxy/config.xml

Locate the first <ssl> block and set its content to the following:

```
<ssl>
    <!-- The server private key file -->
    <privateKey>/etc/vmware-rhttpproxy/ssl/rui.key</privateKey>
    <!-- The server side certificate file -->
    <certificate>/etc/vmware-rhttpproxy/ssl/rui.crt</certificate>
    <!-- vecs server name. Currently vecs runs on all node types. -->
    <vecsServerName>localhost</vecsServerName>
</ssl>
```

Restart the service for changes to take effect.

```
# vmon-cli --restart rhttpproxy
```

Additional Information:

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)

1.7 VCRP-70-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy (rhttpproxy) log files must be shipped via syslog to a central log server.

```
GROUP ID: V-256743
RULE ID: SV-256743r889167
```

Rationale:

Envoy produces several logs that must be offloaded from the originating system. This information can then be used for diagnostic purposes, forensics purposes, or other purposes relevant to ensuring the availability and integrity of the hosted application.

Envoy (rhttpproxy) rsyslog configuration is included in the "VMware-visl-integration" package and unpacked to "/etc/vmware-syslog/vmware-services-rhttpproxy.conf". Ensuring the package hashes are as expected also ensures the shipped rsyslog configuration is present and unmodified.

Audit:

At the command prompt, run the following command:

```
# rpm -V VMware-visl-integration|grep vmware-services-rhttpproxy.conf|grep
"^..5....."
```

If the command returns any output, 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")
```

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)

1.8 VCRP-70-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Envoy log files must be shipped via syslog to a central log server.

```
GROUP ID: V-256744
RULE ID: SV-256744r889170
```

Rationale:

Envoy rsyslog configuration is included in the "VMware-visl-integration" package and unpacked to "/etc/vmware-syslog/vmware-services-envoy.conf". Ensuring the package hashes are as expected also ensures the shipped rsyslog configuration is present and unmodified.

Audit:

At the command prompt, run the following command:

```
# rpm -V VMware-visl-integration|grep vmware-services-envoy.conf|grep
"^..5......"
```

If the command returns any output, 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")
```

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)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCRP-70-000001 (Manual)	☐	☐
1.2	VCRP-70-000002 (Manual)	☐	☐
1.3	VCRP-70-000003 (Manual)	☐	☐
1.4	VCRP-70-000004 (Manual)	☐	☐
1.5	VCRP-70-000005 (Manual)	☐	☐
1.6	VCRP-70-000006 (Manual)	☐	☐
1.7	VCRP-70-000007 (Manual)	☐	☐
1.8	VCRP-70-000008 (Manual)	☐	☐

Appendix: Change History

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