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

Version: 1 Release: 2 Benchmark

Date: 26 Jul 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 STS 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 STS

Recommendations

1 STIG RULES

VMware vSphere 7.0

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

Version: 1 Release: 2 Benchmark

Date: 26 Jul 2023

CLASSIFICATION unclassified

1.1 VCST-70-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must limit the amount of time that each Transmission Control Protocol (TCP) connection is kept alive.

```
GROUP ID: V-256745
RULE ID: SV-256745r889205
```

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.

In Tomcat, the "connectionTimeout" attribute sets the number of milliseconds the server will wait after accepting a connection for the requested Uniform Resource Identifier (URI) line to be presented. This timeout will also be used when reading the request body (if any). This prevents idle sockets that are not sending HTTP requests from consuming system resources and potentially denying new connections.

Audit:

At the command prompt, run the following command:

```
#  xmllint --xpath '/Server/Service/Connector[@port="${bio-
custom.http.port}"]/@connectionTimeout' /usr/lib/vmware-sso/vmware-
sts/conf/server.xml
```

Expected result:

connectionTimeout="60000"

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Navigate to each of the `<Connector>` nodes.

Configure each `<Connector>` node with the value:

connectionTimeout="60000"

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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 VCST-70-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must limit the number of concurrent connections permitted.

```
GROUP ID: V-256746
RULE ID: SV-256746r889208
```

Rationale:

Resource exhaustion can occur when an unlimited number of concurrent requests are allowed on a website, facilitating a denial-of-service attack. Unless the number of requests is controlled, the web server can consume enough system resources to cause a system crash.

Mitigating this kind of attack will include limiting the number of concurrent HTTP/HTTPS requests. In Tomcat, each incoming request requires a thread for the duration of that request. If more simultaneous requests are received than can be handled by the currently available request processing threads, additional threads will be created up to the value of the "maxThreads" attribute.

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath
'/Server/Service/Executor[@name="tomcatThreadPool"]/@maxThreads'
/usr/lib/vmware-sso/vmware-sts/conf/server.xml
```

Expected result:

maxThreads="150"

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Navigate to the <Executor> mode with the name of "tomcatThreadPool" and configure with the value 'maxThreads="150"' as follows:

```
<Executor maxThreads="150" minSpareThreads="50" name="tomcatThreadPool"
namePrefix="tomcat-http--" />
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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 VCST-70-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must limit the maximum size of a POST request.

```
GROUP ID: V-256747
RULE ID: SV-256747r889211
```

Rationale:

The "maxPostSize" value is the maximum size in bytes of the POST that will be handled by the container FORM URL parameter parsing. Limit its size to reduce exposure to a denial-of-service (DoS) attack.

If "maxPostSize" is not set, the default value of 2097152 (2MB) is used. Security Token Service is configured in its shipping state to not set a value for "maxPostSize".

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath '/Server/Service/Connector[@port="${bio-
custom.http.port}"]/@maxPostSize' /usr/lib/vmware-sso/vmware-
sts/conf/server.xml
```

Expected result:

XPath set is empty

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Navigate to each of the `<Connector>` nodes.

Remove any configuration for "maxPostSize".

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

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

1.4 VCST-70-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must protect cookies from cross-site scripting (XSS).

```
GROUP ID: V-256748
RULE ID: SV-256748r889214
```

Rationale:

Cookies are a common way to save session state over the HTTP(S) protocol. If an attacker can compromise session data stored in a cookie, they are better able to launch an attack against the server and its applications.

When a cookie is tagged with the "HttpOnly" flag, it tells the browser that this particular cookie should only be accessed by the originating server. Any attempt to access the cookie from client script is strictly forbidden.

Satisfies: SRG-APP-000001-WSR-000002, SRG-APP-000223-WSR-000011, SRG-APP-000439-WSR-000154

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/session-config/cookie-
config/http-only' -
```

Expected result:

```
<http-only>true</http-only>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Navigate to the <session-config> node and configure it as follows:

```
<session-config>
        <session-timeout>30</session-timeout>
        <cookie-config>
            <http-only>true</http-only>
            <secure>true</secure>
       </cookie-config>
</session-config>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

CCI-001664 Recognize only session identifiers that are system-generated.

- NIST SP 800-53::SC-23 (3)
- NIST SP 800-53A::SC-23 (3).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

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

1.5 VCST-70-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must record user access in a format that enables monitoring of remote access.

```
GROUP ID: V-256749
RULE ID: SV-256749r889217
```

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.

Tomcat can be configured with an "AccessLogValve", a component that can be inserted into the request processing pipeline to provide robust access logging. The "AccessLogValve" creates log files in the same format as those created by standard web servers. When "AccessLogValve" is properly configured, log files will contain all the forensic information necessary in the case of a security incident.

Satisfies: SRG-APP-000016-WSR-000005, SRG-APP-000093-WSR-000053, SRG-APP-000095-WSR-000056, SRG-APP-000096-WSR-000057, SRG-APP-000097-WSR-000058, SRG-APP-000098-WSR-000059, SRG-APP-000098-WSR-000060, 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:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/server.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath
'/Server/Service/Engine/Host/Valve[@className="org.apache.catalina.valves.Acc
essLogValve"]/@pattern' -
```

Expected result:

pattern="%t %I [RemoteIP] %{X-Forwarded-For}i %u [Request] %h:%{remote}p to local %{local}p - %H %m %U%q [Response] %s - %b bytes [Perf] process %Dms / commit %Fms / conn [%X]"

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Inside the <Host> node, find the "AccessLogValve" <Valve> node and replace the "pattern" element as follows:

pattern="%t %I [RemoteIP] %{X-Forwarded-For}i %u [Request] %h:%{remote}p to local %{local}p - %H %m %U%q [Response] %s - %b bytes [Perf] process %Dms / commit %Fms / conn [%X]"

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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)

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-001462 The information system provides the capability for authorized users to capture/record and log content related to a user session.

- NIST SP 800-53::AU-14 a
- NIST SP 800-53A::AU-14.1 (i)
- NIST SP 800-53 Revision 4::AU-14 (2)

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

1.6 VCST-70-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must generate log records during Java startup and shutdown.

```
GROUP ID: V-256750
RULE ID: SV-256750r918974
```

Rationale:

Logging must be started as soon as possible when a service starts and as late as possible when a service is stopped. Many forms of suspicious actions can be detected by analyzing logs for unexpected service starts and stops. Also, by starting to log immediately after a service starts, it becomes more difficult for suspicious activity to go unlogged.

Satisfies: SRG-APP-000089-WSR-000047, SRG-APP-000092-WSR-000055

Audit:

At the command prompt, run the following command:

```
# grep "1catalina.org.apache.juli.FileHandler" /usr/lib/vmware-sso/vmware-
sts/conf/logging.properties
```

Expected result:

```
handlers = 1catalina.org.apache.juli.FileHandler,
2localhost.org.apache.juli.FileHandler, 3manager.org.apache.juli.FileHandler,
4host-manager.org.apache.juli.FileHandler
.handlers = 1catalina.org.apache.juli.FileHandler
1catalina.org.apache.juli.FileHandler.level = FINE
1catalina.org.apache.juli.FileHandler.directory =
${catalina.base}/logs/tomcat
1catalina.org.apache.juli.FileHandler.prefix = catalina.
1catalina.org.apache.juli.FileHandler.bufferSize = -1
1catalina.org.apache.juli.FileHandler.formatter =
java.util.logging.SimpleFormatter
1catalina.org.apache.juli.FileHandler.maxDays = 10
org.apache.catalina.startup.Catalina.handlers =
1catalina.org.apache.juli.FileHandler
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/logging.properties

Ensure that the "handlers" and ".handlers" lines are configured as follows:

```
handlers = 1catalina.org.apache.juli.FileHandler,
2localhost.org.apache.juli.FileHandler, 3manager.org.apache.juli.FileHandler,
4host-manager.org.apache.juli.FileHandler
.handlers = 1catalina.org.apache.juli.FileHandler
1catalina.org.apache.juli.FileHandler.level = FINE
1catalina.org.apache.juli.FileHandler.directory =
${catalina.base}/logs/tomcat
1catalina.org.apache.juli.FileHandler.prefix = catalina.
1catalina.org.apache.juli.FileHandler.bufferSize = -1
1catalina.org.apache.juli.FileHandler.formatter =
java.util.logging.SimpleFormatter
1catalina.org.apache.juli.FileHandler.maxDays = 10
org.apache.catalina.startup.Catalina.handlers =
1catalina.org.apache.juli.FileHandler
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

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

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

1.7 VCST-70-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Security Token Service log files must only be modifiable by privileged users.

```
GROUP ID: V-256751
RULE ID: SV-256751r889223
```

Rationale:

Log data is essential in the investigation of events. The accuracy of the information is always pertinent. One of the first steps an attacker will undertake is the modification or deletion of log records to cover tracks and prolong discovery.

The web server must protect the log data from unauthorized modification. Security Token Service restricts all modification of log files by default, but this configuration must be verified.

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

Audit:

At the command prompt, run the following command:

```
# find /storage/log/vmware/sso/ -xdev -type f -a '(' -perm -o+w -o -not -user
root -o -not -group root ')' -exec ls -ld {} \;
```

If any files are returned, this is a finding.

Remediation:

At the command prompt, run the following commands:

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

Note: Substitute `<file>` with the listed file.

Additional Information:

CCI-000163 Protect audit information from unauthorized modification.

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

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

1.8 VCST-70-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service application files must be verified for their integrity.

```
GROUP ID: V-256752
RULE ID: SV-256752r889226
```

Rationale:

Verifying the Security Token Service application code is unchanged from its shipping state is essential for file validation and nonrepudiation of the Security Token Service. There is no reason the MD5 hash of the RPM original files should be changed after installation, excluding configuration files.

Satisfies: SRG-APP-000131-WSR-000051, SRG-APP-000357-WSR-000150

Audit:

At the command prompt, run the following command:

```
# rpm -V vmware-identity-sts|grep "^..5......"|grep -v -E
"\.properties|\.xml|\.conf"
```

If there is any output, this is a finding.

Remediation:

Reinstall the vCenter Server Appliance (VCSA) or roll back to a backup.

VMware does not support modifying the Security Token Service installation files manually.

Additional Information:

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

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

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

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

1.9 VCST-70-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must only run one webapp.

```
GROUP ID: V-256753
RULE ID: SV-256753r889229
```

Rationale:

VMware ships the Security Token Service on the vCenter Server Appliance (VCSA) with one webapp, in "ROOT.war". Any other ".war" file is potentially malicious and must be removed.

Satisfies: SRG-APP-000131-WSR-000073, SRG-APP-000141-WSR-000075

Audit:

At the command prompt, run the following command:

```
# ls /usr/lib/vmware-sso/vmware-sts/webapps/*.war
```

Expected result:

/usr/lib/vmware-sso/vmware-sts/webapps/ROOT.war

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

Remediation:

For each unexpected file returned in the check, run the following command:

```
# rm /usr/lib/vmware-sso/vmware-sts/webapps/<NAME>.war
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

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

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

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

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

1.10 VCST-70-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must not be configured with unused realms.

```
GROUP ID: V-256754
RULE ID: SV-256754r889232
```

Rationale:

The Security Token Service performs user authentication at the application level and not through Tomcat. To eliminate unnecessary features and ensure the Security Token Service remains in its shipping state, the lack of a "UserDatabaseRealm" configuration must be confirmed.

Audit:

At the command prompt, run the following command:

```
# grep UserDatabaseRealm /usr/lib/vmware-sso/vmware-sts/conf/server.xml
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Remove the `<Realm>` node returned in the check.

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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 VCST-70-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must be configured to limit access to internal packages.

```
GROUP ID: V-256755
RULE ID: SV-256755r889235
```

Rationale:

The "package.access" entry in the "catalina.properties" file implements access control at the package level. When properly configured, a Security Exception will be reported if an errant or malicious webapp attempts to access the listed internal classes directly or if a new class is defined under the protected packages.

The Security Token Service comes preconfigured with the appropriate packages defined in "package.access", and this configuration must be maintained.

Audit:

At the command prompt, run the following command:

```
# grep "package.access" /usr/lib/vmware-sso/vmware-
sts/conf/catalina.properties
```

Expected result:

package.access=sun.,org.apache.catalina.,org.apache.coyote.,org.apache.tomcat.,org.apache.jasper.

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/catalina.properties

Ensure the "package.access" line is configured as follows:

package.access=sun.,org.apache.catalina.,org.apache.coyote.,org.apache.tomcat.,org.apache.jasper.

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.12 VCST-70-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must have Multipurpose Internet Mail Extensions (MIME) that invoke operating system shell programs disabled.

```
GROUP ID: V-256756
RULE ID: SV-256756r889238
```

Rationale:

MIME mappings tell the Security Token Service what type of program various file types and extensions are and what external utilities or programs are needed to execute the file type.

By ensuring various shell script MIME types are not included in "web.xml", the server is protected against malicious users tricking the server into executing shell command files.

Audit:

At the command prompt, run the following command:

```
# grep -En '(x-csh<)|(x-sh<)|(x-shar<)|(x-ksh<)' /usr/lib/vmware-sso/vmware-
sts/conf/web.xml
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Remove all of the following nodes lines:

```
<mime-type>application/x-csh</mime-type>
<mime-type>application/x-shar</mime-type>
<mime-type>application/x-sh</mime-type>
<mime-type>application/x-ksh</mime-type>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Note: Delete the entire mime-mapping node for the target mime-type.

Example:

```
<mime-mapping>
    <extension>sh</extension>
    <mime-type>application/x-sh</mime-type>
</mime-mapping>
```

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

1.13 VCST-70-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must have mappings set for Java servlet pages.

```
GROUP ID: V-256757
RULE ID: SV-256757r889241
```

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 identify which file types are not to be delivered to a client.

By not specifying which files can and cannot be served to a user, the web server could deliver to a user web server configuration files, log files, password files, etc.

As Tomcat is a Java-based web server, the main file extension used is *.jsp. This check ensures the *.jsp and *.jspx file types have been properly mapped to servlets.

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/servlet-mapping/servlet-
name[text()="jsp"]/parent::servlet-mapping' -
```

Expected result:

```
<servlet-mapping>
    <servlet-name>jsp</servlet-name>
    <url-pattern>*.jsp</url-pattern>
    <url-pattern>*.jspx</url-pattern>
</servlet-mapping>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Inside the <web-app> parent node, add the following:

```
<servlet-mapping>
    <servlet-name>jsp</servlet-name>
    <url-pattern>*.jsp</url-pattern>
    <url-pattern>*.jspx</url-pattern>
</servlet-mapping>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.14 VCST-70-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must not have the Web Distributed Authoring (WebDAV) servlet installed.

```
GROUP ID: V-256758
RULE ID: SV-256758r889244
```

Rationale:

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

Tomcat uses the "org.apache.catalina.servlets.WebdavServlet" servlet to provide WebDAV services. Because the WebDAV service has been found to have an excessive number of vulnerabilities, this servlet must not be installed. The Security Token Service does not configure WebDAV by default.

Audit:

At the command prompt, run the following command:

```
# grep -n 'webdav' /usr/lib/vmware-sso/vmware-sts/conf/web.xml
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Find the <servlet-name>webdav</servlet-name> node and remove the entire parent <servlet> block.

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.15 VCST-70-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must be configured with memory leak protection.

```
GROUP ID: V-256759
RULE ID: SV-256759r889247
```

Rationale:

The Java Runtime environment can cause a memory leak or lock files under certain conditions. Without memory leak protection, the Security Token Service can continue to consume system resources which will lead to "OutOfMemoryErrors" when reloading web applications.

Memory leaks occur when JRE code uses the context class loader to load a singleton. This this will cause a memory leak if a web application class loader happens to be the context class loader at the time. The "JreMemoryLeakPreventionListener" class is designed to initialize these singletons when Tomcat's common class loader is the context class loader. Proper use of JRE memory leak protection will ensure the hosted application does not consume system resources and cause an unstable environment.

Audit:

At the command prompt, run the following command:

```
# grep JreMemoryLeakPreventionListener /usr/lib/vmware-sso/vmware-
sts/conf/server.xml
```

Expected result:

```
<Listener
className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Navigate to the <Server> node.

Add '<Listener
className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>' to the
<Server> node.

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.16 VCST-70-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must not have any symbolic links in the web content directory tree.

```
GROUP ID: V-256760
RULE ID: SV-256760r889250
```

Rationale:

A web server is designed to deliver content and execute scripts or applications on the request of a client or user. Containing user requests to files in the directory tree of the hosted web application and limiting the execution of scripts and applications guarantees the user is not accessing information protected outside the application's realm.

By checking that no symbolic links exist in the document root, the web server is protected from users jumping outside the hosted application directory tree and gaining access to the other directories, including the system root.

Audit:

At the command prompt, run the following command:

```
# find /usr/lib/vmware-sso/vmware-sts/webapps/ -type l -ls
```

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

Remediation:

At the command prompt, run the following command:

Note: Replace `<file_name>` for the name of any files that were returned.

```
# unlink <file_name>
```

Repeat the command for each file that was returned.

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

1.17 VCST-70-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service directory tree must have permissions in an out-of-the-box state.

```
GROUP ID: V-256761
RULE ID: SV-256761r889253
```

Rationale:

As a rule, accounts on a web server are to be kept to a minimum. Only administrators, web managers, developers, auditors, and web authors require accounts on the machine hosting the web server. The resources to which these accounts have access must also be closely monitored and controlled. The Security Token Service files must be adequately protected with correct permissions as applied out of the box.

Satisfies: SRG-APP-000211-WSR-000030, SRG-APP-000380-WSR-000072

Audit:

At the command prompt, run the following command:

```
# find /usr/lib/vmware-sso/vmware-sts/ -xdev -type f -a '(' -not -user root -
o -not -group root ')' -exec ls -ld {} \;
```

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

Remediation:

At the command prompt, run the following command:

```
# chown root:root <file_name>
```

Repeat the command for each file that was returned.

Note: Replace `<file_name>` for the name of the file that was returned.

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

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

1.18 VCST-70-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must fail to a known safe state if system initialization fails, shutdown fails, or aborts fail.

```
GROUP ID: V-256762
RULE ID: SV-256762r889256
```

Rationale:

Determining a safe state for failure and weighing that against a potential denial of service for users depends on what type of application the web server is hosting. For the Security Token Service, it is preferable that the service abort startup on any initialization failure rather than continuing in a degraded, and potentially insecure, state.

Audit:

At the command line, run the following command:

```
# grep EXIT_ON_INIT_FAILURE /usr/lib/vmware-sso/vmware-
sts/conf/catalina.properties
```

Expected result:

org.apache.catalina.startup.EXIT_ON_INIT_FAILURE=true

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/catalina.properties

Add or change the following line:

org.apache.catalina.startup.EXIT_ON_INIT_FAILURE=true

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

CCI-001190 Fail to an organization-defined known-system state for the list of organization-defined types of system failures on organization-defined system components on the indicated components while preserving organization-defined system state information in failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (iv)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-24

1.19 VCST-70-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must set "URIEncoding" to UTF-8.

```
GROUP ID: V-256764
RULE ID: SV-256764r889262
```

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 characters into hosted applications in an effort to break out of the document home or root home directory or bypass security checks. The Security Token Service must be configured to use a consistent character set via the "URIEncoding" attribute on the Connector nodes.

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath '/Server/Service/Connector[@port="${bio-
custom.http.port}"]/@URIEncoding' /usr/lib/vmware-sso/vmware-
sts/conf/server.xml
```

Expected result:

URIEncoding="UTF-8"

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Navigate to each of the <Connector> nodes.

Configure each <Connector> node with the value 'URIEncoding="UTF-8"'.

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.20 VCST-70-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must limit the number of allowed connections.

```
GROUP ID: V-256763
RULE ID: SV-256763r889259
```

Rationale:

Limiting the number of established connections to the Security Token Service is a basic denial-of-service protection. Servers where the limit is too high or unlimited can potentially run out of system resources and negatively affect system availability.

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath '/Server/Service/Connector[@port="${bio-
custom.http.port}"]/@acceptCount' /usr/lib/vmware-sso/vmware-
sts/conf/server.xml
```

Expected result:

acceptCount="100"

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Navigate to the `<Connector>` configured with port="${bio-custom.http.port}".

Add or change the following value:

acceptCount="100"

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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)

1.21 VCST-70-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must use the "setCharacterEncodingFilter" filter.

```
GROUP ID: V-256765
RULE ID: SV-256765r889265
```

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 characters into hosted applications in an effort to break out of the document home or root home directory or to bypass security checks. VMware uses the standard Tomcat "SetCharacterEncodingFilter" to provide a layer of defense against character encoding attacks. Filters are Java objects that perform filtering tasks on the request to a resource (a servlet or static content), on the response from a resource, or both.

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/filter-mapping/filter-
name[text()="setCharacterEncodingFilter"]/parent::filter-mapping' -
```

Expected result:

```
<filter-mapping>
    <filter-name>setCharacterEncodingFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

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

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/filter/filter-
name[text()="setCharacterEncodingFilter"]/parent::filter' -
```

Expected result:

```
   <filter>
      <filter-name>setCharacterEncodingFilter</filter-name>
      <filter-class>
         org.apache.catalina.filters.SetCharacterEncodingFilter
      </filter-class>
      <init-param>
         <param-name>encoding</param-name>
         <param-value>UTF-8</param-value>
      </init-param>
      <init-param>
         <param-name>ignore</param-name>
         <param-value>true</param-value>
      </init-param>
      <async-supported>true</async-supported>
   </filter>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Configure the node with the child nodes listed below:

```
<filter-mapping>
    <filter-name>setCharacterEncodingFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>

   <filter>
      <filter-name>setCharacterEncodingFilter</filter-name>
      <filter-class>
         org.apache.catalina.filters.SetCharacterEncodingFilter
      </filter-class>
      <init-param>
         <param-name>encoding</param-name>
         <param-value>UTF-8</param-value>
      </init-param>
      <init-param>
         <param-name>ignore</param-name>
         <param-value>true</param-value>
      </init-param>
      <async-supported>true</async-supported>
   </filter>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.22 VCST-70-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must set the welcome-file node to a default web page.

```
GROUP ID: V-256766
RULE ID: SV-256766r889268
```

Rationale:

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. Ensuring every document directory has an "index.jsp" (or equivalent) file is one approach to mitigating the vulnerability.

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/welcome-file-list' -
```

Expected result:

```
<welcome-file-list>
    <welcome-file>index.html</welcome-file>
    <welcome-file>index.htm</welcome-file>
    <welcome-file>index.jsp</welcome-file>
</welcome-file-list>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Add the following section under the <web-apps> node:

```
<welcome-file-list>
    <welcome-file>index.html</welcome-file>
    <welcome-file>index.htm</welcome-file>
    <welcome-file>index.jsp</welcome-file>
</welcome-file-list>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.23 VCST-70-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must not show directory listings.

```
GROUP ID: V-256767
RULE ID: SV-256767r889271
```

Rationale:

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. Ensuring directory listing is disabled is one approach to mitigating the vulnerability.

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '//param-
name[text()="listings"]/parent::init-param' -
```

Expected result:

```
<init-param>
      <param-name>listings</param-name>
      <param-value>false</param-value>
</init-param>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Set the <param-value> to "false" in all <param-name>listing</param-name> nodes.

Note: The setting should look like the following:

```
<init-param>
      <param-name>listings</param-name>
      <param-value>false</param-value>
</init-param>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.24 VCST-70-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must be configured to not show error reports.

```
GROUP ID: V-256768
RULE ID: SV-256768r889274
```

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, the Security Token Service must be configured to not show server version information in error messages.

Audit:

At the command prompt, run the following command:

```
# xmllint --xpath
'/Server/Service/Engine/Host/Valve[@className="org.apache.catalina.valves.Err
orReportValve"]' /usr/lib/vmware-sso/vmware-sts/conf/server.xml
```

Expected result:

```
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showReport="false" showServerInfo="false"/>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Locate the following Host block:

```
<Host ...>
...
</Host>
```

Inside this block, remove any existing Valve with className="org.apache.catalina.valves.ErrorReportValve" and add the following:

```
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showServerInfo="false" showReport="false"/>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.25 VCST-70-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must not enable support for TRACE requests.

```
GROUP ID: V-256769
RULE ID: SV-256769r889277
```

Rationale:

"TRACE" is a technique for a user to request internal information about Tomcat. This is useful during product development but should not be enabled in production. Allowing an attacker to conduct a TRACE operation against the Security Token Service will expose information that would be useful to perform a more targeted attack.

The Security Token Service provides the "allowTrace" parameter as means to disable responding to TRACE requests.

Audit:

At the command prompt, run the following command:

```
# grep allowTrace /usr/lib/vmware-sso/vmware-sts/conf/server.xml
```

If "allowTrace" is set to "true", this is a finding.

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/server.xml

Locate and remove the 'allowTrace="true"' setting.

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.26 VCST-70-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must have the debug option disabled.

```
GROUP ID: V-256770
RULE ID: SV-256770r918976
```

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.

The Security Token Service can be configured to set the debugging level. By setting the debugging level to zero, no debugging information will be provided to a malicious user.

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '//param-
name[text()="debug"]/parent::init-param' -
```

Expected result:

```
<init-param>
    <param-name>debug</param-name>
    <param-value>0</param-value>
</init-param>
```

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

If no lines are returned, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Navigate to all nodes that are not set to "0".

Set the `<param-value>` to "0" in all `<param-name>debug</param-name>` nodes.

Note: The debug setting should look like the following:

```
<init-param>
    <param-name>debug</param-name>
    <param-value>0</param-value>
</init-param>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.27 VCST-70-000028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must be configured with the appropriate ports.

```
GROUP ID: V-256771
RULE ID: SV-256771r918979
```

Rationale:

Web servers provide numerous processes, features, and functionalities that use TCP/IP ports. Some of these processes may be deemed unnecessary or too unsecure to run on a production system. The ports that the Security Token Service listens on are configured in the "catalina.properties" file and must be verified as accurate to their shipping state.

Audit:

At the command prompt, run the following command:

```
# grep 'bio' /usr/lib/vmware-sso/vmware-sts/conf/catalina.properties
```

Expected result:

```
bio-custom.http.port=7080
bio-custom.https.port=8443
bio-ssl-clientauth.https.port=3128
bio-ssl-localhost.https.port=7444
```

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

Note: Port 3128 will not be shown in the output prior to 7.0 U3i.

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/catalina.properties

Navigate to the ports specification section.

Set the Security Token Service port specifications according to the following list:

```
bio-custom.http.port=7080
bio-custom.https.port=8443
bio-ssl-clientauth.https.port=3128
bio-ssl-localhost.https.port=7444
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.28 VCST-70-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must disable the shutdown port.

```
GROUP ID: V-256772
RULE ID: SV-256772r889286
```

Rationale:

An attacker has at least two reasons to stop a web server. The first is to cause a denial of service, and the second is to put in place changes the attacker made to the web server configuration.

If the Tomcat shutdown port feature is enabled, a shutdown signal can be sent to the Security Token Service through this port. To ensure availability, the shutdown port must be disabled.

Audit:

At the command prompt, run the following command:

```
# grep 'base.shutdown.port' /usr/lib/vmware-sso/vmware-
sts/conf/catalina.properties
```

Expected result:

base.shutdown.port=-1

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/catalina.properties

Add or modify the following setting:

base.shutdown.port=-1

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

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

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

1.29 VCST-70-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service must set the secure flag for cookies.

```
GROUP ID: V-256773
RULE ID: SV-256773r889289
```

Rationale:

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of the cookie in clear text.

By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel. The Security Token Service is configured to only be accessible over a Transport Layer Security (TLS) tunnel, but this cookie flag is still a recommended best practice.

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/session-config/cookie-
config/secure' -
```

Expected result:

```
<secure>true</secure>
```

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Navigate to the /<web-apps>/<session-config>/<cookie-config> node and configure it as follows:

```
    <cookie-config>
      <http-only>true</http-only>
      <secure>true</secure>
    </cookie-config>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

Additional Information:

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

1.30 VCST-70-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Token Service default servlet must be set to "readonly".

```
GROUP ID: V-256774
RULE ID: SV-256774r889292
```

Rationale:

The default servlet (or DefaultServlet) is a special servlet provided with Tomcat that is called when no other suitable page is found in a particular folder. The DefaultServlet serves static resources as well as directory listings.

The DefaultServlet is configured by default with the "readonly" parameter set to "true" where HTTP commands such as PUT and DELETE are rejected. Changing this to "false" allows clients to delete or modify static resources on the server and to upload new resources.

DefaultServlet readonly must be set to "true", either literally or by absence (default).

Audit:

At the command prompt, run the following command:

```
# xmllint --format /usr/lib/vmware-sso/vmware-sts/conf/web.xml | sed '2
s/xmlns=".*"//g' | xmllint --xpath '/web-app/servlet/servlet-
name[text()="default"]/../init-param/param-name[text()="readonly"]/../param-
value[text()="false"]' -
```

Expected result:

XPath set is empty

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

Remediation:

Navigate to and open:

/usr/lib/vmware-sso/vmware-sts/conf/web.xml

Navigate to the /<web-apps>/<servlet>/<servlet-name>default</servlet-name>/ node and remove the following node:

```
<init-param>
      <param-name>readonly</param-name>
      <param-value>false</param-value>
</init-param>
```

Restart the service with the following command:

```
# vmon-cli --restart sts
```

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

1.31 VCST-70-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Security Token Service log data and records must be backed up onto a different system or media.

```
GROUP ID: V-256775
RULE ID: SV-256775r889295
```

Rationale:

Protection of Security Token Service log data includes ensuring log data is not accidentally lost or deleted. Backing up Security Token Service log records to an unrelated system or onto separate media than the system the web server is running on helps to ensure 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-000163

Audit:

At the command prompt, run the following command:

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

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

Remediation:

Navigate to and open:

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

Create the file if it does not exist.

Set the contents of the file as follows:

```
#vmidentity logs
input(type="imfile"
      File="/var/log/vmware/sso/activedirectoryservice.log"
      Tag="activedirectoryservice"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}Z"
      Facility="local0")
input(type="imfile"
      File="/var/log/vmware/sso/lookupsvc-init.log"
      Tag="ssolookupsvc-init"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}Z"
      Facility="local0")
input(type="imfile"
      File="/var/log/vmware/sso/openidconnect.log"
      Tag="openidconnect"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}Z"
      Facility="local0")
input(type="imfile"
      File="/var/log/vmware/sso/ssoAdminServer.log"
      Tag="ssoadminserver"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}Z"
      Facility="local0")
input(type="imfile"
      File="/var/log/vmware/sso/svcaccountmgmt.log"
      Tag="svcaccountmgmt"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}Z"
      Facility="local0")
input(type="imfile"
      File="/var/log/vmware/sso/tokenservice.log"
      Tag="tokenservice"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}Z"
      Facility="local0")
#sts health log
input(type="imfile"
```

```
      File="/var/log/vmware/sso/sts-health-status.log.*"
      Tag="sts-health-status"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-[[:digit:]]{1,2}
[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2},[[:digit:]]{0,4}"
      Facility="local0")
#sts runtime log
input(type="imfile"
      File="/var/log/vmware/sso/sts-runtime.log.*"
      Tag="sts-runtime"
      PersistStateInterval="200"
      Severity="info"
      Facility="local0")
#gclogFile.0.current log
input(type="imfile"
      File="/var/log/vmware/sso/gclogFile.*.current"
      Tag="gclog"
      PersistStateInterval="200"
      Severity="info"
      startmsg.regex="^[[:digit:]]{4}-[[:digit:]]{1,2}-
[[:digit:]]{1,2}T[[:digit:]]{1,2}:[[:digit:]]{1,2}:[[:digit:]]{1,2}.[[:digit:
]]{0,3}+[[:digit:]]{0,4}"
      Facility="local0")
#tomcat log
input(type="imfile"
      File="/var/log/vmware/sso/tomcat/localhost_access.log"
      Tag="sso-tomcat"
      PersistStateInterval="200"
      Severity="info"
      Facility="local0")
#vmdir log
input(type="imfile"
      File="/var/log/vmware/vmdir/*.log"
      Tag="vmdir"
      PersistStateInterval="200"
      Severity="info"
      Facility="local0")
#vmafd log
input(type="imfile"
      File="/var/log/vmware/vmafd/*.log"
      Tag="vmafd"
      PersistStateInterval="200"
      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)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCST-70-000001 (Manual)	☐	☐
1.2	VCST-70-000002 (Manual)	☐	☐
1.3	VCST-70-000003 (Manual)	☐	☐
1.4	VCST-70-000004 (Manual)	☐	☐
1.5	VCST-70-000005 (Manual)	☐	☐
1.6	VCST-70-000006 (Manual)	☐	☐
1.7	VCST-70-000007 (Manual)	☐	☐
1.8	VCST-70-000008 (Manual)	☐	☐
1.9	VCST-70-000009 (Manual)	☐	☐
1.10	VCST-70-000010 (Manual)	☐	☐
1.11	VCST-70-000011 (Manual)	☐	☐
1.12	VCST-70-000012 (Manual)	☐	☐
1.13	VCST-70-000013 (Manual)	☐	☐
1.14	VCST-70-000014 (Manual)	☐	☐
1.15	VCST-70-000015 (Manual)	☐	☐
1.16	VCST-70-000016 (Manual)	☐	☐
1.17	VCST-70-000017 (Manual)	☐	☐
1.18	VCST-70-000018 (Manual)	☐	☐
1.19	VCST-70-000020 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	VCST-70-000019 (Manual)	☐	☐
1.21	VCST-70-000021 (Manual)	☐	☐
1.22	VCST-70-000022 (Manual)	☐	☐
1.23	VCST-70-000023 (Manual)	☐	☐
1.24	VCST-70-000024 (Manual)	☐	☐
1.25	VCST-70-000025 (Manual)	☐	☐
1.26	VCST-70-000026 (Manual)	☐	☐
1.27	VCST-70-000028 (Manual)	☐	☐
1.28	VCST-70-000029 (Manual)	☐	☐
1.29	VCST-70-000030 (Manual)	☐	☐
1.30	VCST-70-000031 (Manual)	☐	☐
1.31	VCST-70-000050 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 21, 2025	1.0.0	Initial CIS Release