CIS IBM WebSphere Liberty Server STIG Benchmark

v1.0.0 – 04-02-2025

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

IBM WebSphere Liberty Server Secure Technical Implementation Guide (STIG)
Version: 2 Release: 2 Benchmark
Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate IBM WebSphere Liberty Server 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 IBM WebSphere Liberty Server

Recommendations

1 STIG RULES

IBM Websphere Liberty

IBM WebSphere Liberty Server Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 IBMW-LS-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Maximum in-memory session count must be set according to application requirements.

```
GROUP ID: V-250322
RULE ID: SV-250322r960735
```

Rationale:

Application management includes the ability to control the number of sessions that use an application by all accounts and/or account types. Limiting the number of allowed sessions is helpful in limiting risks related to Denial of Service attacks.

Application servers host and expose business logic and application processes. The application server must possess the capability to limit the maximum number of concurrent sessions in a manner that affects the entire application server or on an individual application basis. Although there is some latitude concerning the settings themselves, the settings should follow DoD-recommended values, but the settings should be configurable to allow for future DoD direction. While the DoD will specify recommended values, the values can be adjusted to accommodate the operational requirement of a given system.

The System Security Plan should be reviewed and the maximum number of concurrent sessions allowable and defined within that plan should be used in the httpSession element. For example, if the maximum number of concurrent sessions is defined in the System Security Plan as 5000, then the httpSession element in ${server.config.dir}/server.xml should be configured as: <httpSession maxInMemorySessionCount="5000" allowOverflow="false" />

For http session security settings to apply, the security feature (appSecurity-2.0) must be defined in order to configure a user registry for the servlet to authenticate against. The servlet feature (servlet-3.1) must be defined in order to use a web application, and the ldap feature (ldapRegistry-3.0) must be defined in order to configure an enterprise-level user registry for authentication of the servlet users.

Audit:

Review the System Security plan to determine the maximum number of concurrent sessions allowed. This is a per user setting and must be defined by the application admins.
As a privileged user with access to the server.xml file, review file content and identify the "maxInMemorySessionCount" and the allowOverflow settings.
EXAMPLE:
grep -i maxInMemorySessionCount server.xml

If maxInMemorySessionCount is not set in server.xml according to the settings defined in the system security plan or if allowOverflow="true", this is a finding.

Remediation:

To limit the max number of concurrent sessions available, the ${server.config.dir}/server.xml must be configured with maxInMemorySessionCount set according to system security plan and allowOverflow="false".
EXAMPLE:
<httpSession maxInMemorySessionCount="5" allowOverflow="false" />

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 IBMW-LS-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server Quality of Protection (QoP) must be set to use TLSv1.2 or higher.

```
GROUP ID: V-250323
RULE ID: SV-250323r960759
```

Rationale:

Quality of Protection in WebSphere Liberty specifies the security level, ciphers, and mutual authentication settings for the Secure Socket Layer (SSL/TLS) configuration. For Quality of Protection settings to apply, the security feature (appSecurity-2.0) must be defined in order to configure a user registry for the servlet to authenticate against. The SSL feature (ssl-1.0) must be defined in order to configure ssl settings, and the ldap feature (ldapRegistry-3.0) must be defined in order to configure an enterprise-level user registry for authentication of users.

Audit:

As a privileged user with local file access to ${server.config.dir}/server.xml, verify the appSecurity-x.x feature and the sslProtocol settings are configured.
grep -i appsecurity- server.xml
RESULT:
appSecurity-2.0
Verify the SSL protocol setting is configured for TLSV1.2 for every SSL configuration. There can be multiple SSL configurations and SSL ID settings.
grep -i "<ssl id=" server.xml
SAMPLE RESULT:
<ssl id="TLSSettings" keyStoreRef="TLSKeyStore" trustStoreRef="TLSTrustStore" sslProtocol="TLSv1.2"/>
If the SSL protocol setting does not specify TLS v.1.2 or higher, or if the appSecurity feature is not configured, this is a finding.

Remediation:

To ensure the QoP is set to TLS v1.2 or higher, the ${server.config.dir}/server.xml file must be configured as follows:
<featureManager>appSecurity-2.0ssl-1.0</featureManager>
For every SSL configuration, the sslProtocol field must be set to TLS v1.2 or higher.

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)

1.3 IBMW-LS-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Security cookies must be set to HTTPOnly.

```
GROUP ID: V-250324
RULE ID: SV-250324r960762
```

Rationale:

Web applications use cookies to track users across requests. These cookies, while typically not sensitive in themselves, connect to the existing state on the back-end system. If an intruder were to capture one of these cookies, they could potentially use the cookie to act as the user. Important web traffic should be encrypted using SSL. This includes important cookies.

In the case of WebSphere Liberty Server, the most important cookies are the LTPA cookie and session cookie; therefore, both should be configured to be only sent over SSL. To set httpOnly on the application server's cookies, the security feature (appSecurity-2.0) must be defined in order to configure a user registry for the servlet to authenticate against. The servlet (servlet-3.1) feature must be defined in order to deploy web applications, the ssl (ssl-1.0) feature must be defined in order to do SSL communications, and the ldap feature (ldapRegistry-3.0) must be defined in order to configure an enterprise-level user registry for authentication of users.

For the LTPA cookie, the httpOnlyCookies element must be set to true:
<webAppSecurity ssoCookieName="LtpaToken2" ssoRequiresSSL="true" httpOnlyCookies="true" logoutOnHttpSessionExpire="true"/>

For the JSESSIONID cookie, the cookieHttpOnly element must be set to true:
<httpSession cookieName="JSESSIONID" cookieSecure="true" cookieHttpOnly="true" cookiePath="/"/>

Audit:

As a user with local file access to ${server.config.dir}/server.xml, verify appSecurity feature is enabled.
<featureManager>appSecurity-2.0</featureManager>
Verify both web application LTPA and http session cookies are configured for httpOnly.

If the appSecurity feature is not enabled or if the LPTA or Session cookie settings are not set for httpOnly, this is a finding.

Remediation:

To ensure security cookies use httpOnly, the ${server.config.dir)/server.xml must be configured as follows:
<featureManager>appSecurity-2.0</featureManager>

Additional Information:

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

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

1.4 IBMW-LS-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must log remote session and security activity.

```
GROUP ID: V-250325
RULE ID: SV-250325r1015250
```

Rationale:

Security auditing must be configured in order to log remote session activity. Security auditing will not be performed unless the audit feature (audit-1.0) has been enabled. The security feature (appSecurity-2.0) must be enabled for the security auditing to capture security transactions. Remote session activity will then be logged, regardless of the user attempting that activity.

Satisfies: SRG-APP-000016-AS-000013, SRG-APP-000080-AS-000045, SRG-APP-000089-AS-000050, SRG-APP-000091-AS-000052, SRG-APP-000095-AS-000056, SRG-APP-000096-AS-000059, SRG-APP-000097-AS-000060, SRG-APP-000098-AS-000061, SRG-APP-000099-AS-000062, SRG-APP-000100-AS-000063, SRG-APP-000101-AS-000072, SRG-APP-000266-AS-000168, SRG-APP-000343-AS-000030, SRG-APP-000172-AS-000121

Audit:

Review the ${server.config.dir}/server.xml file and ensure audit-1.0 and appSecurity-2.0 are defined within the <featureManager> setting in the server.xml file.
If audit-1.0 and appSecurity-2.0 are not defined within the <featureManager> setting in the server.xml file, this is a finding.
EXAMPLE:
<featureManager>
audit-1.0
appSecurity-3.0
</featureManager>

Remediation:

To log remote access events, the featureManager setting in the ${server.config.dir}/server.xml must contain the audit and appSecurity features.

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-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

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

CCI-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-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

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

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

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

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-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

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-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)
- NIST SP 800-53 Revision 5::AC-6 (9)

1.5 IBMW-LS-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Users in the REST API admin role must be authorized.

```
GROUP ID: V-250326
RULE ID: SV-250326r960792
```

Rationale:

Users with console access and OS permissions to the folders where the Liberty Server is installed can make changes to the server. In addition, REST API calls that execute server management tasks are available and can be executed remotely. Adding a user to the admin role will allow that user to make changes to the server via the REST API calls.

The admin role must be controlled and users who are in that role must be authorized.

Audit:

As a user with access to ${server.config.dir}/server.xml, review the file and look for the admin role settings.
grep -i administrator-role ${server.config.dir}/server.xml
grep -i quickstartsecurity ${server.config.dir}/server.xml
If the admin role has been created, users in that role must be documented and approved. However, using the basic registry or the quickstartsecurity methods are not acceptable. The preferred user registry method is to use a centralized access control method via LDAP.
If no admin users exist at all, this is not a finding.
If admin users in an LDAP user registry configuration are not documented and approved, this is a finding.
If admin users exist in a basic user registry configuration, or in a quickstartsecurity user configuration, this is a finding.
LDAP EXAMPLE:

cn=bob,o=ibm,c=us

BASIC REGISTRY EXAMPLE:
<basicRegistry>

<group name="group1" ...>

</basicRegistry>

QUICKSTARTSECURITY EXAMPLE:
<featureManager>
restConnector-2.0
</featureManager>
<quickStartSecurity userName="bob" userPassword="bobpassword" />
<keyStore id="defaultKeyStore" password="keystorePassword"/>

Remediation:

If an admin user exists in either a basic user registry or a quickstartsecurity registry, edit the ${server.config.dir}/server.xml file and remove the basic registry and/or quickstartsecurity registry settings.
If an admin user exists via an LDAP user registry setting, document and approve the user(s) or group that have been assigned to the admin role and ensure anyone granted REST API admin rights is authorized.
LDAP EXAMPLE:

cn=bob,o=ibm,c=us

BASIC REGISTRY EXAMPLE:
<basicRegistry>

<group name="group1" ...>

</basicRegistry>

QUICKSTARTSECURITY EXAMPLE:
<featureManager>
restConnector-2.0
</featureManager>
<quickStartSecurity userName="bob" userPassword="bobpassword" />
<keyStore id="defaultKeyStore" password="keystorePassword"/>

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

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

1.6 IBMW-LS-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must be configured to offload logs to a centralized system.

```
GROUP ID: V-250327
RULE ID: SV-250327r1043188
```

Rationale:

Log processing failures include, but are not limited to, failures in the application server log capturing mechanisms or log storage capacity being reached or exceeded. In some instances, it is preferred to send alarms to individuals rather than to an entire group. Application servers must be able to trigger an alarm and send an alert to, at a minimum, the SA and ISSO in the event there is an application server log processing failure.

Satisfies: SRG-APP-000109-AS-000070, SRG-APP-000358-AS-000064

Audit:

As a privileged user with local file access to ${server.config.dir}/server.xml, verify the logstashCollector-1.0 feature is enabled.
grep -i -A5 logstashcollector server.xml
EXAMPLE:
<featureManager>
logstashCollector-1.0
</featureManager>
<logstashCollector source="message,accessLog,audit"
hostName=""
port=""
sslRef="DefaultTLSSettings"
</logstashCollector>
If "logstashCollector" is not a configured feature and the logstashCollector "source" setting does not contain "message,accessLog,audit", this is a finding.

Remediation:

To send Liberty logs to a centralized syslog system, the Elastic environment must be set up as per the ELK stack/Elasticsearch directions. Once that is completed, configure the server.xml. The following is a sample configuration. Individual keystore, truststore, and authentication settings will vary. The SME must substitute their own values as needed.
The message, audit, and accessLog sources must be included at a minimum.
For additional information refer to the IBM website:
https://www.ibm.com/support/knowledgecenter/SSEQTP_liberty/com.ibm.WebSphere.wlp.doc/ae/twlp_analytics_logstash.html
EXAMPLE:

<logstashCollector
source="message,accessLog,audit"
hostName="your ELK stack server"
port="Your ELK stack port"
sslRef="myTLSConfig">
</logstashCollector>

Additional Information:

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

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

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

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

1.7 IBMW-LS-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must protect log information from unauthorized access or changes.

```
GROUP ID: V-250328
RULE ID: SV-250328r960933
```

Rationale:

WebSphere Liberty provides the capability to encrypt and sign the log data to prevent unauthorized modification.

- The security feature (appSecurity-2.0) must be defined in order to configure a user registry for the servlet to authenticate against.
- The audit feature (audit-1.0) must be defined in order to generate audit records.
- The servlet feature (servlet-3.1) must be defined to be able to deploy a web application.
- The ejb feature (ejbLite-3.1) must be defined to be able to deploy an ejb application.
- The ssl feature (ssl-1.0) must be defined to be able to generate and use certificates to sign and encrypt logs.
- The ldap feature (ldapRegistry-3.0) must be defined in order to configure an enterprise-level user registry to authenticate users against.

When the audit-1.0 feature is defined, all supported audit events will be captured and logged to an audit.log located under ${server.config.dir}/logs.

The audit log that is currently being logged to is called audit.log. When an audit log fills to a configured maximum capacity, it is archived with a timestamp with the naming convention audit_.log and new records are written to audit.log.

The audit logs are found under the ${server.config.dir}/logs directory and are named audit.log for the most recent, and audit_.log for any archived logs.

Two keystores need to be created (ikeyman as part of the JDK may be used) and a personal certificate created in each. One keystore will contain the certificate used to encrypt the logs; the other keystore will contain the certificate used to sign the logs. The audit configuration needs to define the location of these two keystores, their passwords, and the alias of each certificate used to encrypt and sign the logs. As an example:
<keyStore id="auditEncKeyStore" password="Liberty"
location="${server.config.dir}/resources/security/AuditEncryptionKeyStore.jks"
type="JKS" />

```
  <keyStore
     id="auditSignKeyStore"
     password="{xor}EzY9Oi0rJg=="

location="${server.config.dir}/resources/security/AuditSigningKeyStore2.jks"
     type="JKS" />
```

<auditFileHandler encrypt="true" encryptAlias="auditencryption" encryptKeyStoreRef="auditEncKeyStore" sign="true" signingAlias="auditsigning2" signingKeyStoreRef="auditSignKeyStore"> </auditFileHandler>

Satisfies: SRG-APP-000119-AS-000079, SRG-APP-000120-AS-000080

Audit:

As a user with local file access to ${server.config.dir}/logs, verify the following audit log files have the correct file permissions of 660.
audit.log
messages.log
console.log
trace.log (if it exists)
If the file permissions for these files are not set to 660, this is a finding.

Remediation:

As a user with local file access to ${server.config.dir}/logs, use the chmod command to configure the following log files to have the correct file permissions of 660.
chmod 660 <filename.log>
audit.log
messages.log
console.log
trace.log (if it exists)

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 IBMW-LS-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must protect log tools from unauthorized access.

```
GROUP ID: V-250329
RULE ID: SV-250329r960939
```

Rationale:

Protecting log data also includes identifying and protecting the tools used to view and manipulate log data. Depending on the log format and application, system and application log tools may provide the only means to manipulate and manage application and system log data. Therefore, it is imperative that access to log tools be controlled and protected from unauthorized access.

Application servers provide a web- and/or a command line-based management functionality for managing the application server log capabilities. In addition, subsets of log tool components may be stored on the file system as jar or xml configuration files. The application server must ensure that in addition to protecting any web-based log tools, any file system-based tools are protected as well.

Audit:

As a user with local file access to the /opt/IBM/WebSphere/Liberty/bin folder, verify the following audit tool files have the correct file permissions of 755.
binaryLog
auditUtility
If the file permissions for these files are not set to 755, this is a finding.

Remediation:

As a user with local file access to the /opt/IBM/WebSphere/Liberty/bin/ folder, use the chmod command to configure the correct file permissions of 755 for the following files.
binaryLog
auditUtility

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

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

1.9 IBMW-LS-000320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must be configured to encrypt log information.

```
GROUP ID: V-250330
RULE ID: SV-250330r960951
```

Rationale:

Protection of log records is of critical importance. Encrypting log records provides a level of protection that does not rely on host-based protections that can be accidentally misconfigured, such as file system permissions. Cryptographic mechanisms are the industry-established standard used to protect the integrity of log data. An example of a cryptographic mechanism is the computation and application of a cryptographic-signed hash using asymmetric cryptography.

- The security feature (appSecurity-2.0) must be defined in order to configure a user registry for the servlet to authenticate against.
- The audit feature (audit-1.0) must be defined in order to generate audit records.
- The servlet feature (servlet-3.1) must be defined to be able to deploy a web application.
- The ejb feature (ejbLite-3.1) must be defined to be able to deploy an ejb application.
- The ssl feature (ssl-1.0) must be defined to be able to generate and use certificates to sign and encrypt logs.
- The ldap feature (ldapRegistry-3.0) must be defined in order to configure an enterprise-level user registry to authenticate users against.

When the audit-1.0 feature is defined, all supported audit events will be captured and logged to an audit.log located under ${server.config.dir}/logs.

The audit log that is currently being logged to is called audit.log. When an audit log fills to a configured maximum capacity, it is archived with a timestamp with the naming convention audit_.log and new records are written to audit.log.

The audit logs are found under the ${server.config.dir}/logs directory and are named audit.log for the most recent, and audit_.log for any archived logs.

One keystore needs to be created (ikeyman as part of the JDK may be used) and a personal certificate created. This certificate is used to encrypt the logs. The audit configuration needs to define the location of this keystore, its password, and the alias of the certificate used to encrypt the logs. As an example:
<keyStore id="auditEncKeyStore" password="Liberty" location="${server.config.dir}/resources/security/AuditEncryptionKeyStore.jks" type="JKS" />

```
  <keyStore
     id="auditSignKeyStore"
     password="{xor}EzY9Oi0rJg=="

location="${server.config.dir}/resources/security/AuditSigningKeyStore2.jks"
     type="JKS" />
```

<auditFileHandler encrypt="true" encryptAlias="auditencryption" encryptKeyStoreRef="auditEncKeyStore" </auditFileHandler>

Satisfies: SRG-APP-000126-AS-000085, SRG-APP-000118-AS-000078, SRG-APP-000267-AS-000170

Audit:

If the system is configured to send logs to a remote ELK stack log server, as per requirement IBMW-LS-000230, (or other remote logging solution) this requirement is Not Applicable.
As a user with local file access to ${server.config.dir}/server.xml:

1. Verify the following features are configured.

2. Verify a keystore is configured. The following is an example:

<keyStore
id="auditEncKeyStore"
password="ENTER THE ENCRYPTION KEYSTORE PASSWORD"
location="${server.config.dir}/resources/security/AuditEncryptionKeyStore.jks"
type="JKS" />

```
  <keyStore
     id="auditSignKeyStore"
     password="ENTER THE SIGNING KEYSTORE PASSWORD"

location="${server.config.dir}/resources/security/AuditSigningKeyStore2.jks"
     type="JKS" />
```

3. Verify auditFileHandler encryption is enabled. Signing is optional.

<auditFileHandler
encrypt="true"
encryptAlias="auditencryption"
encryptKeyStoreRef="auditEncKeyStore"
sign="true"
signingAlias="auditsigning2"
signingKeyStoreRef="auditSignKeyStore">
</auditFileHandler>
If the features and keystore are not configured, and encryption is not enabled, this is a finding.

Remediation:

If the system is configured to send logs to a remote ELK stack log server, (or other remote logging solution) as per requirement IBMW-LS-000230, this requirement is Not Applicable.
Signing is optional. The encrypted and/or signed audit logs are found under the ${server.config.dir}/logs directory and are named audit.log for the most recent, and audit_.log for any archived logs. Two keystores are recommended but not required when doing both encryption and signing (ikeyman as part of the JDK may be used) and a certificate imported into each. One keystore will contain the certificate used to encrypt the logs; the other keystore will contain the certificate used to sign the logs. The audit configuration must define the location of every keystore, their passwords, and the alias of each certificate used to encrypt and sign the logs.

1. Enable the following features:

2. Verify a keystore is configured. The following is a JKS keystore example. PKCS12 is also a viable keystore:

<keyStore
id="auditEncKeyStore"
password="ENTER THE ENCRYPTION KEYSTORE PASSWORD"
location="${server.config.dir}/resources/security/AuditEncryptionKeyStore.jks"
type="JKS" />

```
  <keyStore
     id="auditSignKeyStore"
     password="ENTER THE SIGNING KEYSTORE PASSWORD"

location="${server.config.dir}/resources/security/AuditSigningKeyStore2.jks"
     type="JKS" />
```

3. Enable auditFileHandler encryption. Signing the logs is optional.

<auditFileHandler
encrypt="true"
encryptAlias="auditencryption"
encryptKeyStoreRef="auditEncKeyStore"
sign="true"
signingAlias="auditsigning2"
signingKeyStoreRef="auditSignKeyStore">
</auditFileHandler>

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-001314 Reveal error messages only to organization-defined personnel or roles.

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

CCI-001350 Implement cryptographic mechanisms to protect the integrity of audit information.

- NIST SP 800-53::AU-9 (3)
- NIST SP 800-53A::AU-9 (3).1
- NIST SP 800-53 Revision 4::AU-9 (3)
- NIST SP 800-53 Revision 5::AU-9 (3)

1.10 IBMW-LS-000340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must protect software libraries from unauthorized access.

```
GROUP ID: V-250331
RULE ID: SV-250331r960960
```

Rationale:

Application servers have the ability to specify that the hosted applications use shared libraries. The application server must have a capability to divide roles based upon duties wherein one project user (such as a developer) cannot modify the shared library code of another project user. The application server must also be able to specify that non-privileged users cannot modify any shared library code at all.

Audit:

As a privileged user with local file access to the /opt/IBM/WebSphere/Liberty/lib/ folder, verify all of the jar files in the lib folder have the correct file permissions of 664.
If the file permissions for all jar files in the lib folder are not set to 664, this is a finding.

Remediation:

As a privileged user with local file access to the /opt/IBM/WebSphere/Liberty/lib/ folder, verify all of the jar files in the lib folder have the correct file permissions of 664.
If the file permissions for all jar files in the lib folder are not set to 664, use the chmod command to change the file permissions.
chmod 664 *.jar

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.11 IBMW-LS-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must prohibit or restrict the use of nonsecure ports, protocols, modules, and/or services as defined in the PPSM CAL and vulnerability assessments.

```
GROUP ID: V-250332
RULE ID: SV-250332r1043177
```

Rationale:

Some networking protocols may not meet organizational security requirements to protect data and components.

Application servers natively host a number of various features, such as management interfaces, httpd servers, and message queues. These features all run on TCPIP ports. This creates the potential that the vendor may choose to use port numbers or network services that have been deemed unusable by the organization. The application server must have the capability to both reconfigure and disable the assigned ports without adversely impacting application server operation capabilities. For a list of approved ports and protocols, reference the DoD ports and protocols website at https://powhatan.iiie.disa.mil/ports/cal.html.

Audit:

As a privileged user with access to the server.xml file, review the file and identify all TCPIP ports used by the server.
EXAMPLE:
grep -I "port=" server.xml
httpsPort="9443">
Review the PPSM site for the list of approved ports. If any of the ports used are not registered with PPSM, this is a finding.

Remediation:

Every port listed in ${server.config.dir}/server.xml must be registered with PPSM. Refer to the PPSM website on https://cyber.mil/ppsm for information.

Additional Information:

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

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

1.12 IBMW-LS-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must use an LDAP user registry.

```
GROUP ID: V-250333
RULE ID: SV-250333r1051118
```

Rationale:

To ensure accountability and prevent unauthorized access, application server users must be uniquely identified and authenticated. This is typically accomplished via the use of a user store which is either local (OS-based) or centralized (LDAP) in nature. Best practice guideline to is to use a centralized enterprise LDAP server.

To ensure support to the enterprise, the authentication must use an enterprise solution.

Audit:

As a user with local file access to ${server.config.dir}/server.xml file, verify the LDAP user registry is used to authenticate users. If the LDAP user registry is not defined within server.xml, this is a finding.

<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
ldapType="${ldap.vendor.type}"
searchTimeout="8m">
</ldapRegistry>

Remediation:

To ensure an enterprise user management system is configured to uniquely identify and authenticate users and processes acting on behalf of org users, the server.xml must be configured to use an ldap configuration as follows:

<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
ldapType="${ldap.vendor.type}"
searchTimeout="8m">
</ldapRegistry>

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

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

1.13 IBMW-LS-000381 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Basic Authentication must be disabled.

```
GROUP ID: V-250334
RULE ID: SV-250334r1051118
```

Rationale:

Basic authentication does not use a centralized user store like LDAP. Not using a centralized user store complicates user management tasks and increases the risk that user accounts could remain on the system long after users have moved to their next deployment. Basic Auth also stores user credentials and passwords on the system and creates the potential for an attacker to circumvent strong authentication requirements like multi-factor or certificate based authentication.

Allowing failover to Basic Auth allows the Liberty Server to fall back to basic authentication in the event certificate based authentication methods fail. Configuring the Liberty Server to fall back to basic authentication creates the potential for an attacker to circumvent strong authentication requirements and must be avoided.

Audit:

As a privileged user with local file access to the ${server.config.dir}/server.xml file, search the server.xml for the basicRegistry setting.
grep -i basicregistry server.xml
SAMPLE:
<basicRegistry id="basic" realm="BasicRealm">

</basicRegistry>
If <basicRegistry> settings are defined in server.xml, this is a finding.

Remediation:

Delete basicRegistry settings and re-configure the server.xml file to use a centralized LDAP user store.
SAMPLE:

<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
ldapType="${ldap.vendor.type}"
searchTimeout="8m">
</ldapRegistry>

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

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

1.14 IBMW-LS-000390 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Multifactor authentication for network access to privileged accounts must be used.

```
GROUP ID: V-250335
RULE ID: SV-250335r1015469
```

Rationale:

Multifactor authentication creates a layered defense and makes it more difficult for an unauthorized person to access the application server. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Unlike a simple username/password scenario where the attacker could gain access by knowing both the username and password without the user knowing his account was compromised, multifactor authentication adds the requirement that the attacker must have something from the user, such as a token, or to biometrically be the user.

When accessing the application server via a network connection, administrative access to the application server must be PKI Hardware Token enabled.

The high level steps required for configuring Liberty Server to use certificate based authentication include the following:

1. Configure Web Application with client certificate authentication.
2. Configure Liberty SSL configuration with client authentication.
3. Configure Liberty LDAP Security Configuration with certificate filter.

Satisfies: SRG-APP-000149-AS-000102, SRG-APP-000151-AS-000103, SRG-APP-000402-AS-000247, SRG-APP-000403-AS-000248, SRG-APP-000177-AS-000126

Audit:

As a user with local file access to ${server.config.dir}/server.xml file, verify the TLS connection used for managing the server is configured to use clientAuthentication.

Verify the TLS connection used for managing the server is configured to use clientAuthentication. The following is used as an example.
If the clientAuthentication setting for the TLS management application is not set to "true", this is a finding.
EXAMPLE:

```
<sslDefault sslRef="defaultSSLSettings" />
<ssl id="defaultSSLSettings" keyStoreRef="defaultKeyStore"
sslProtocol="SSL_TLSv2" trustStoreRef="defaultTrustStore"
```

clientAuthentication="true"/>
Access the web management interface via a web browser and verify TLS secured connectivity to the web based management application.

Remediation:

Refer to IBM documentation on how to configure TLS and client based certificate authentication for additional configuration details. The following is a summary list of items needed to configure the system for certificate based authentication. Production systems and installations will vary.
The application's web.xml file must be configured to use client certs.
EXAMPLE:

CLIENT-CERT

The server.xml features must be configured to use transportSecurity and an ldap configuration.

The server.xml TLS and LDAP settings must be configured. The following is an EXAMPLE only. "Default" verbiage and keystore information in the below SSL configuration will be different in production systems.

```
<sslDefault sslRef="defaultSSLSettings" />
<ssl id="defaultSSLSettings" keyStoreRef="defaultKeyStore"
sslProtocol="SSL_TLSv2" trustStoreRef="defaultTrustStore"
```

clientAuthentication="true"/>

Configure LDAP certificate filter settings according the certificates being used.
<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
ldapType="${ldap.vendor.type}"
certificateMapMode="Certificate_Filter" or "Exact_DN"
certificateFilter="${your certificate mapping}"
searchTimeout="8m"
sslEnabled="true">
</ldapRegistry>

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

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

CCI-000765 Implement multifactor authentication for access to privileged accounts.

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

CCI-002009 Accept Personal Identity Verification-compliant credentials from other federal agencies.

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

CCI-002010 Electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

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

1.15 IBMW-LS-000440 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The WebSphere Liberty Server must store only encrypted representations of user passwords.

```
GROUP ID: V-250336
RULE ID: SV-250336r1015470
```

Rationale:

WebSphere Liberty can either provide a local account store or integrate with enterprise account stores such as LDAP directories. If the application server stores application passwords in the server.xml configuration files, the application server must store encrypted representations of passwords rather than unencrypted, clear-text passwords.

The Liberty Application Server provides a SecurityUtility tool that can take a plain-text or encoded password and convert it to an encrypted password. This tool does not update the ${server.config.dir/server.xml file directly; a manual update of the server.xml is needed once the utility is run.

It is imperative that administrators understand that the SecurityUtility tool must be run for each application password that is stored within the server.xml file.

Satisfies: SRG-APP-000171-AS-000119, SRG-APP-000428-AS-000265, SRG-APP-000429-AS-000157

Audit:

As a privileged user with file access to ${server.config.dir}/server.xml, review and ensure there are no clear-text passwords stored within the server.xml file.
If any passwords appear in plain text, or if any passwords start with {xor}, this is a finding.

Remediation:

For additional information regarding the use of the SecurityUtility command, refer to IBM's website:
https://www.ibm.com/docs/en/was-liberty/base?topic=applications-securityutility-command
Create a new xml file with file permissions of 660.
File owner and group membership is the same as the WebSphere Liberty server user.
Add the following line to the new xml file:

In the above, "mysecret" is the passphrase selected to create a cryptographic hash that represents the password.
Save the file to a secured location. Note the path and name, as it will be needed when updating server.xml.
Edit the server.xml file and add the following line:

For every unencrypted password in server.xml, run the following SecurityUtility command, which can be found in the Liberty Server install path:
SecurityUtility encode --encoding=aes
This will prompt the user to enter the plain-text password stored within the server.xml file.
The SecurityUtility tool will generate an AES cryptographic hash of the password.
Copy and replace the plain-text password with the hashed value.
This must be done for every plain-text password in server.xml.
Restart the server by entering:
server stop
server start

Additional Information:

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

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

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

1.16 IBMW-LS-000450 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The WebSphere Liberty Server must use TLS-enabled LDAP.

```
GROUP ID: V-250337
RULE ID: SV-250337r961029
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords during transmission. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Application servers have the capability to use either certificates (tokens) or user IDs and passwords in order to authenticate. When the application server transmits or receives passwords, the passwords must be encrypted. The certificate used by LDAP to establish trust with incoming client requests must be imported into a trust keystore created on the Liberty Server (JDK ikeyman may be used to do this). The LDAP configuration must indicate it is using SSL, provide the BindDN and BindPassword and point to the trust keystore containing the LDAP certificate.

Audit:

As a user with local file access to ${server.config.dir}/server.xml, verify TLS-enabled LDAP is in use. If TLS-Enabled LDAP is not defined within server.xml, this is a finding.

<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
bindDN="${ldap.server.bind.dn}’
bindPassword="${ldap.server.bind.password}"
sslEnabled="true"
sslRef="LDAPTLSSettings"
ldapType="${ldap.vendor.type}"
searchTimeout="8m">
</ldapRegistry>

Remediation:

To ensure the Liberty Server transmits only encrypted passwords, the ${server.config.dir}/server.xml must be configured as follows:

<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
bindDN="${ldap.server.bind.dn}’
bindPassword="${ldap.server.bind.password}"
sslEnabled="true"
sslRef="LDAPTLSSettings"
ldapType="${ldap.vendor.type}"
searchTimeout="8m">
</ldapRegistry>

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)

1.17 IBMW-LS-000500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must use DoD-issued/signed certificates.

```
GROUP ID: V-250338
RULE ID: SV-250338r961044
```

Rationale:

The cornerstone of PKI is the private key used to encrypt or digitally sign information. The key by itself is a cryptographic value that does not contain specific user information, but the key can be mapped to a user. Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Satisfies: SRG-APP-000177-AS-000126, SRG-APP-000427-AS-000264, SRG-APP-000514-AS-000137

Audit:

As a privileged user with access to the ${server.config.dir}/server.xml file; search for SSLDefault in order to identify the default SSL configuration.
grep -i ssldefault server.xml
Identify the default ssl configuration by examining the sslRef flag.
SAMPLE:
<sslDefault sslRef="DefaultTLSSettings" />
Review the default ssl configuration to identify the default truststore.
SAMPLE:
<ssl id="DefaultTLSSettings" keyStoreRef="defaultKeyStore" />
<keyStore id="LDAPTrustStore" location="${server.config.dir}/liberty.ks" type="JKS" password="xxxxxxx" />
Use the java keytool or ikeyman utilities to open and examine the certificates stored in the truststore.
If the certificates are self signed or not signed by a DoD approved CA, this is a finding.

Remediation:

Do not use self-signed certificates in a production environment. Only import certificates signed by an authorized DoD CA or authorized for DoD use.
Obtain the signer certificate either as a Base 64-encoded ASCII file or as binary DER data.
Using the JDK’s ikeyman or keytool utility, open the default trusted keystore specified in the ${server.config.dir}/server.xml.
Click on signer certificates and import the file that contains the DoD signed certificate.

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

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

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

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

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

1.18 IBMW-LS-000520 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The WebSphere Liberty Server must use FIPS 140-2 approved encryption modules when authenticating users and processes.

```
GROUP ID: V-250339
RULE ID: SV-250339r1067571
```

Rationale:

Application servers must use and meet requirements of the DOD Enterprise PKI infrastructure for application authentication. Encryption is only as good as the encryption modules used. Unapproved cryptographic module algorithms cannot be verified and cannot be relied upon to provide confidentiality or integrity, and DOD data may be compromised due to weak algorithms. The use of TLS provides confidentiality of data in transit between the application server and client.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Satisfies: SRG-APP-000179-AS-000129, SRG-APP-000224-AS-000152, SRG-APP-000416-AS-000140, SRG-APP-000439-AS-000155, SRG-APP-000442-AS-000259, SRG-APP-000514-AS-000136

Audit:

There are two ways to meet this requirement. Only one method is required.
If IBM JDK 8 is installed and configured to run with WebSphere Liberty, proceed with method (I).
If IBM Semeru Runtimes version 11 and above is installed and configured with WebSphere Liberty, proceed with method (II). Currently IBM Semeru supports FIPS on RedHat Enterprise Linux.
Method (I) IBM JDK 8 is configured to run with WebSphere Liberty:

1. Review the ${server.config.dir}/jvm.options file. Verify FIPS is in use by checking the following lines:

Dcom.ibm.jsse2.usefipsprovider=true
Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS
If the properties are not set as shown in the ${server.config.dir}/jvm.options file, this is a finding.

2. Open ${JAVA_HOME}/jre/lib/security/java.security file. Locate the list of cryptographic providers and confirm the following entries in the provider list:

com.ibm.crypto.plus.provider.IBMJSSEProvider2
com.ibm.crypto.plus.provider.IBMJCEPlusFIPS
com.ibm.crypto.plus.provider.IBMJCEPlus
com.ibm.crypto.plus.provider.IBMJCE
If the entries are not set as shown in the ${JAVA_HOME}/jre/lib/security/java.security file, this is a finding.
Method (II) Semeru Runtimes version 11 and above is installed and configured with WebSphere Liberty. Requires RedHat Enterprise Linux as the Host Operating System.

1. Run the following command on the RedHat Enterprise Linux. Verify FIPS mode is enabled.

fips-mode-setup --check

If FIPS mode is not enabled, this is a finding.

2. Review the ${server.config.dir}/jvm.options file. Verify "semeru.fips" property is set to true.
   Dsemeru.fips=true
   If the property is not set as shown in the ${server.config.dir}/jvm.options file, this is a finding.

3. Confirm NSS packages are installed by running "# dnf install nss" in a terminal.

dnf install nss

Updating Subscription Management repositories.
Last metadata expiration check: 0:56:30 ago on Wed 13 Sep 2023 07:29:35 AM PDT.
Package nss-3.79.0-11.el8_7.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
If the command does not return output stating NSS is installed, this is a finding.

4. Confirm NSS Database has the keystore imported by running "# certutil -L -d /etc/pki/nssdb" in a terminal.

certutil -L -d /etc/pki/nssdb

Certificate Nickname Trust Attributes
SSL,S/MIME,JAR/XPI
default CTu,Cu,Cu
If the command does not return the results as shown, this is a finding.

5. Review the ${server.config.dir}/server.xml and confirm the following entries:

name = NSS-FIPS
library = /usr/lib64/libsoftokn3.so
slot = 3
showInfo = true
If the entries are not set as shown in the ${server.config.dir}/server.xml file, this is a finding.

6. Review the ${server.config.dir}/server.xml file with the following steps:

6.1 Locate configuration that is specifying the default SSL configuration for Liberty.
6.2 Locate the "keyStoreRef" attribute in the configuration and find the referenced <keyStore> configuration.
6.3 Verify the "provider" attribute is set to either "SunPKCS11-NSS-FIPS" or "PKCS11-NSS-FIPS" in the <keyStore> configuration.
6.4 Verify the "type" attribute is set to "PKCS11".
6.5 Verify the "fileBased" attribute is set to "false".
6.6 Find the "location" attribute for the configuration file of NSS keystore database (In the example below, it is "/tmp/pkcs11cfg.cfg").
6.7 Verify the file is in a location that is accessible to Liberty.
Snippet of server.xml:
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" sslProtocol="TLSv1.2" />
<keyStore id="defaultKeyStore" password="{xor}Lz4sLCgwLTsINis3" location="/tmp/pkcs11cfg.cfg" type="PKCS11" fileBased="false" provider="SunPKCS11-NSS-FIPS" />
If the entries are not set as shown in the ${server.config.dir}/server.xml file, this is a finding.

Remediation:

There are two ways to meet this requirement. Only one method is required.
If IBM JDK 8 is installed and configured to run with WebSphere Liberty, proceed with method (I).
If IBM Semeru Runtimes version 11 and above is installed and configured with WebSphere Liberty, proceed with method (II). Currently IBM Semeru supports FIPS on RedHat Enterprise Linux.
Method (I) IBM JDK 8 is configured to run with WebSphere Liberty:

1. Edit/Create the ${server.config.dir}/jvm.options file.
   Edit/Add the following two properties:
   Dcom.ibm.jsse2.usefipsprovider=true
   Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS
2. Edit ${JAVA_HOME}/jre/lib/security/java.security file and locate the list of cryptographic providers. Edit/add the following four providers:

security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.plus.provider.IBMJCEPlusFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.crypto.plus.provider.IBMJCEPlus
Method (II) Semeru Runtimes version 11 and above is installed and configured with WebSphere Liberty. Requires RedHat Enterprise Linux as the Host Operating System.

1. Log in as root or super user.
2. Enable FIPS on the RedHat Enterprise Linux.

```
$ fips-mode-setup --enable
$ fips-mode-setup --check
```

3. Update/create the ${server.config.dir}/jvm.options.
   Edit/Add the following property:
   Dsemeru.fips=true
4. Install NSS packages. Run "$ dnf install nss".
5. Import keystores to NSS Database by using "pk12util" command. Replace "changeit" for -W option to the desired password.

```
$ pk12util -i resources/security/key.p12 -W changeit -d /etc/pki/nssdb
```

pk12util: PKCS12 IMPORT SUCCESSFUL

6. Mark the imported certificates as a trusted certificate authority (CA).

```
$ certutil -M -n default -t "CT,CT,CT" -d /etc/pki/nssdb
```

7. List the contents of the NSS Database to confirm the alias name and the Trust Attributes.

```
$ certutil -L -d /etc/pki/nssdb
```

Certificate Nickname Trust Attributes
SSL,S/MIME,JAR/XPI
default CTu,Cu,Cu

8. Create a config file (pkcs11cfg.cfg) with the contents below. It will be used by ${server.config.dir}/server.xml.

name = NSS-FIPS
library = /usr/lib64/libsoftokn3.so
slot = 3
showInfo = true

9. Update the ${server.config.dir}/server.xml file to use the configuration file in its SSL configuration.

<ssl id="defaultSSLConfig"
keyStoreRef="defaultKeyStore"
sslProtocol="TLSv1.2" />

<keyStore id="defaultKeyStore" password="password used in -W parameter earlier here"
location="${server.config.dir}/pkcs11cfg.cfg" type="PKCS11"
fileBased="false" provider="SunPKCS11-NSS-FIPS"/>
9.1 Find the <keyStore/> configuration referenced in the ssl configuration as "keyStoreRef".
9.2 Set "provider" attribute to either "SunPKCS11-NSS-FIPS" or "PKCS11-NSS-FIPS".
9.3 Set the "type" attribute to "PKCS11"
9.4 Set the "fileBased" attribute to "false"
9.5 Set the "location" attribute to point to the NSS keystore configuration created in step 8 (pkcs11.cfg.cfg).
9.6 Verify the file is in a location that is accessible to Liberty.

Additional Information:

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-001188 Generate a unique session identifier for each session with organization-defined randomness requirements.

- NIST SP 800-53::SC-23 (4)
- NIST SP 800-53A::SC-23 (4).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

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

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

CCI-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

1.19 IBMW-LS-000720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

HTTP session timeout must be configured.

```
GROUP ID: V-250340
RULE ID: SV-250340r1043182
```

Rationale:

An attacker can take advantage of user sessions that are left open, thus bypassing the user authentication process.

To thwart the vulnerability of open and unused user sessions, the application server must be configured to close the sessions when a configured condition or trigger event is met.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

Satisfies: SRG-APP-000295-AS-000263, SRG-APP-000389-AS-000253

Audit:

As a user with access to the server xml file, review the contents and verify the httpSession time out setting is configured for 10 minutes.
If the ${server.config.dir}/server.xml does not define the timeout setting as 10 minutes, this is a finding.

Remediation:

The ${server.config.dir}/server.xml file must be configured to update the invalidationTimeout attribute on the httpSession element to set the session timeout value in hours (h) or minutes (m). The server.xml file must define the following:

By default, httpSession invalidationTimeout is set to 30m.

Additional Information:

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

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

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.20 IBMW-LS-000770 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Application security must be enabled on the WebSphere Liberty Server.

```
GROUP ID: V-250341
RULE ID: SV-250341r1015252
```

Rationale:

Application security enables security for the applications in the environment. This type of security provides application isolation and requirements for authenticating application users. When a user enables security, both administrative and application security is enabled.

Application security is in effect only when administrative security is enabled via the security feature. If the application server is to be used for only web applications, only the servlet-3.1 feature needs to be defined. If the application server is to be used for only ejb applications, only the ejbLite-3.1 feature needs to be defined. If both web and ejb applications are to be deployed on the application server, then both the servlet-3.1 and ejbLite-3.1 features need to be defined. The check and fix assumes that the application server will have both web and ejb applications deployed.

Satisfies: SRG-APP-000315-AS-000094, SRG-APP-000014-AS-000009

Audit:

As a user with local file access to ${server.config.dir}/server.xml file, verify application security is enabled.
If the appSecurity-2.0 feature is not defined within server.xml, this is a finding.

Remediation:

Configure the ${server.config.dir}/server.xml file and add the appSecurity-2.0 feature.

Review ${server.config.dir}/logs/messages.log
Validate log entry that indicates "Security service is ready".

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-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)

1.21 IBMW-LS-000790 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Users in a reader-role must be authorized.

```
GROUP ID: V-250342
RULE ID: SV-250342r961353
```

Rationale:

The reader role is a management role that allows read-only access to select administrative REST APIs as well as the Admin Center UI (adminCenter-1.0). Preventing non-privileged users from viewing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Users granted reader role access must be authorized.

Audit:

As a user with access to the ${server.config.dir}/server.xml file. Review the contents and identify if users have been granted the reader-role.
grep -i reader-role ${server.config.dir}/server.xml
If the reader-role has been created, users in that role must be documented and approved.
If users in the reader-role are not approved, this is a finding.
EXAMPLE:
<featureManager>appSecurity-2.0</featureManager>

Remediation:

Edit the ${server.config.dir}/server.xml file. If unauthorized users have been added to the reader-role, remove those users.
Otherwise, document the users who are granted the reader-role access.
To allow read-only access to select administrative REST APIs, the ${server.config.dir}/server.xml must be configured as follows. Additionally, the users and groups they are a part of must be defined within LDAP.
EXAMPLE:
<featureManager>
appSecurity-2.0
</featureManager>

<ldapRegistry id="ldap" realm="SampleLdapRealm" host="${ldap.server.name}"
port="${ldap.server.port}" ignoreCase="true"
baseDN="${ldap.server.base.dn}"
ldapType="${ldap.vendor.type}"
searchTimeout="8m">
</ldapRegistry>

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.22 IBMW-LS-000830 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must allocate JVM log record storage capacity in accordance with organization-defined log record storage requirements.

```
GROUP ID: V-250343
RULE ID: SV-250343r961392
```

Rationale:

JVM logs are logs used to store application and runtime related events, rather than audit related events. They are mainly used to diagnose application or runtime bugs. However, they are useful for providing more context when correlated with audit related events.

By default, Liberty automatically logs the console.log, messages.log, and trace.log but these default settings must be validated.

Audit:

Review the ${server.config.dir}/bootstrap.properties file, verify console logging is not turned off. If the property com.ibm.ws.logging.console.log.level=OFF, this is a finding.
Review the ${server.config.dir}/server.xml file and verify the logging traceSpecification setting is configured according to system capacity requirements. If the logging traceSpecification settings are not configured, this is a finding.
EXAMPLE:
<logging traceSpecification="*=info=enabled:my.package.*=all" maxFileSize="40" maxFiles="20"/>

Remediation:

Edit the bootstrap.properties file and configure the com.ibm.ws.logging.console.log.level=ON.
Edit the ${server.config.dir}/server.xml file. Configure <logging traceSpecification> in accordance with local policy and system storage limits.
EXAMPLE:
<logging traceSpecification="*=info=enabled:my.package.*=all" maxFileSize="40" maxFiles="20"/>,
where maxFileSize is set to the maximum file size defined in local policy and maxFiles is set to the maximum number of historical files defined in local policy and in accordance with system storage limits.

Additional Information:

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

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

1.23 IBMW-LS-000910 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The server.xml file must be protected from unauthorized modification.

```
GROUP ID: V-250344
RULE ID: SV-250344r961461
```

Rationale:

When dealing with access restrictions pertaining to change control, it should be noted that any changes to the software, and/or application server configuration could potentially have significant adverse effects on the overall security of the system.

Protect the server.xml file from unauthorized modification by applying file permission restrictions.

Audit:

As a privileged user with local file access to ${server.config.dir}/server.xml, verify the server.xml file permissions are set to 660.
If the server.xml file permissions are not set to 660, this is a finding.

Remediation:

As a privileged user with local file access to ${server.config.dir}/server.xml.
Use the chmod command to configure the correct file permissions of 660.
chmod 660 server.xml

Additional Information:

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)

1.24 IBMW-LS-000970 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must prohibit the use of cached authenticators after an organization-defined time period.

```
GROUP ID: V-250345
RULE ID: SV-250345r961521
```

Rationale:

Larger authentication cache timeout values can increase security risks. For example, a user who is revoked can still log in by using a credential that is cached in the authentication cache until the cache is refreshed.

Smaller authentication cache timeout values can affect performance. When this value is smaller, the Liberty Server accesses the user registry or repository more frequently.

Larger numbers of entries in the authentication cache, which is caused by an increased number of users, increases the memory usage of the authentication cache. Thus, the application server might slow down and affect performance.

If cached authentication information is out of date, the validity of the authentication information may be questionable.

Audit:

Review system security plan and identify the cache timeout parameters for authentication. The value for admin timeout is 10 minutes. However, a case-by-case exception based on operational requirements can be configured with AO acceptance.
As a privileged user with access to server.xml, review the file and verify the authCache timeout parameter is configured for 10 minutes.
grep -i authcache server.xml
EXAMPLE:
<authCache initialSize="100" maxSize="50000" timeout="10m"/>
If the authCache timeout parameter is not configured for 10 minutes, or the AO has not accepted the risk for extending the timeout period specified, this is a finding.

Remediation:

Edit the server.xml file and define the authCache timeout value as 10 minutes or AO approved value. Also ensure the appSecurity-2.0 feature is enabled.
EXAMPLE:

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

1.25 IBMW-LS-001050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server LTPA keys password must be changed.

```
GROUP ID: V-250346
RULE ID: SV-250346r1067567
```

Rationale:

The default location of the automatically generated Lightweight Third Party Authentication (LTPA) keys file is ${server.output.dir}/resources/security/ltpa.keys.

The LTPA keys are encrypted with a randomly generated key and a default password of WebAS is initially used to protect the keys. The password is required when importing the LTPA keys into another server. To protect the security of the LTPA keys, change the password.

When the LTPA keys are exchanged between servers, this password must match across the servers for Single Sign On (SSO) to work.

Automated LTPA key generation can create unplanned outages. Plan to change the LTPA keys during a scheduled outage and do not use automated key changes. Distribute the new keys to all nodes in the cell and to all external systems/cells during this outage window.

Audit:

If LTPA is not used, this requirement is not a finding.
As a privileged user with access to ${server.config.dir}/server.xml file, review the server.xml file and locate LTPA settings. If the LTPA settings do not exist, this is not a finding.
EXAMPLE:
grep -i "<ltpa" server.xml

If the LTPA setting exists and the password is set to "WebAS", this is a finding.

Remediation:

To update key password and force a regeneration of keys follow these steps. To obtain encoded values, use the Liberty "securityUtility encode" command.

1. Shut down the server.
2. Configure the element in the server.xml file as follows, replacing the sample values in the example with local values. The password may be encoded or encrypted.

3. Delete the existing ${wlp.server.dir}/resources/security/ltpa.keys file.
4. Sync changes with all servers in the cell.
5. Start the servers.

Additional Information:

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

1.26 IBMW-LS-001110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must remove all export ciphers to protect the confidentiality and integrity of transmitted information.

```
GROUP ID: V-250347
RULE ID: SV-250347r961632
```

Rationale:

Export grade encryption suites are not strong and do not meet DoD requirements. The encryption for the session becomes easy for the attacker to break. Do not use export grade encryption.

Audit:

Review the ${server.config.dir}/server.xml file and check the "enabledCiphers" setting. If any of the ciphers specified in the enabledCiphers setting contains the word "EXPORT", this is a finding.
<ssl id="myDefaultSSLConfig"
keyStoreRef="defaultKeyStore"
trustStoreRef="defaultTrustStore"
clientAuthentication="true"
sslProtocol="TLS"
enabledCiphers="SSL_xxx_yyy_zzz"/>

Remediation:

Review the ${server.config.dir}/server.xml file and if needed, modify the "enabledCiphers" setting for each affected SSL configuration.
<ssl id="myDefaultSSLConfig"
keyStoreRef="defaultKeyStore"
trustStoreRef="defaultTrustStore"
clientAuthentication="true"
sslProtocol="TLS"
enabledCiphers="SSL_xxx_yyy_zzz"/>
where xxx, yyy, and zzz do not contain "EXPORT".

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

1.27 IBMW-LS-001120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must be configured to use HTTPS only.

```
GROUP ID: V-250348
RULE ID: SV-250348r961635
```

Rationale:

Transmission of data can take place between the application server and a large number of devices/applications external to the application server. Examples are a web client used by a user, a backend database, a log server, or other application servers in an application server cluster.

Audit:

Review the ${server.config.dir}/server.xml file and check the ssl-1.0 feature and httpEndpoint settings.
If the ssl-1.0 feature is not defined, this is a finding.
If the httpEndpoint settings do not include ssloptions, this is a finding.

<httpEndpoint id="defaultHttpEndpoint"
host="localhost"
httpPort="${bvt.prop.HTTP_default}"
httpsPort="${bvt.prop.HTTP_default.secure}" >
<tcpOptions soReuseAddr="true" />
<sslOptions sslRef="testSSLConfig" />
</httpEndpoint>

Remediation:

Modify the server.xml file. Enable the ssl-1.0 feature and configure the httpEndpoint settings. The keystores and truststores must also be configured.

```
<httpEndpoint id="defaultHttpEndpoint"
      host="localhost"
      httpPort="${bvt.prop.HTTP_default}"
      httpsPort="${bvt.prop.HTTP_default.secure}" >
      <tcpOptions soReuseAddr="true" />
      <sslOptions sslRef="testSSLConfig" />
```

```
 <ssl id="defaultSSLConfig"
  keyStoreRef="defaultKeyStore"
  trustStoreRef="defaultKeyStore"
  serverKeyAlias="default" />

 <ssl id="testSSLConfig"
  keyStoreRef="defaultKeyStore"
  trustStoreRef="alternateTrustStore"
  serverKeyAlias="alternateCert"
  enabledCiphers="AES256-SHA AES128-SHA" />
```

<keyStore id="defaultKeyStore" password="Liberty"
location="${server.config.dir}/resources/security/sslOptions.jks" />
<keyStore id="defaultTrustStore" password="Liberty"
location="${server.config.dir}/resources/security/trust.jks" />
<keyStore id="alternateTrustStore" password="Liberty"
location="${server.config.dir}/resources/security/optionsTrust.jks" />

```
<application type="war" id="basicauth" name="basicauth"
         location="${server.config.dir}/apps/basicauth.war" />
```

Additional Information:

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

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

1.28 IBMW-LS-001170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must install security-relevant software updates within the time period directed by an authoritative source.

```
GROUP ID: V-250349
RULE ID: SV-250349r961683
```

Rationale:

Security vulnerabilities are often addressed by testing and applying the latest security patches and fix packs. The latest fixpacks can be found at: http://www-01.ibm.com/support/docview.wss?uid=swg27009661

Audit:

Use the "productInfo(.bat/.sh) version" command to determine the WebSphere version. Review the patch level and fix pack.
Review the latest fixpacks at: http://www-01.ibm.com/support/docview.wss?uid=swg27009661 and determine if the system is operating at the latest patch level.
If the most recent patches/fix packs have not been applied, this is a finding.

Remediation:

Obtain WebSphere Liberty product security and patch support at http://www-01.ibm.com/support/docview.wss?uid=swg27009661.
Run the productInfo validate command to validate the MD5 checksum file for server installation and each feature.
If a feature is not valid, the command outputs an error and lists the manifest file for the affected feature. The following example validates the features for the current installation and outputs the results to the validate.txt file:
productInfo validate --output=/tmp/validate.txt

Additional Information:

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

1.29 IBMW-LS-001190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The WebSphere Liberty Server must generate log records for authentication and authorization events.

```
GROUP ID: V-250350
RULE ID: SV-250350r961812
```

Rationale:

Enabling authentication (SECURITY_AUTHN) and authorization (SECURITY_AUTHZ) event handlers configures the server to record security authorization and authentication events. By logging these events, the logs can be analyzed to identify activity that could be related to security events and to aid post mortem forensic analysis.

Satisfies: SRG-APP-000499-AS-000224, SRG-APP-000495-AS-000220, SRG-APP-000503-AS-000228, SRG-APP-000504-AS-000229, SRG-APP-000505-AS-000230, SRG-APP-000506-AS-000231, SRG-APP-000509-AS-000234, SRG-APP-000092-AS-000053

Audit:

Review the ${server.config.dir}/server.xml file, verify the audit-1.0 feature is enabled. Also verify the auditFile Handler is configured to log AUTHN and AUTHZ events.
If the audit1.0 feature is not enabled, this is a finding.
If the SECURITY_AUTHN and SECURITY_AUTHZ event handlers are not configured, this is a finding.

```
<auditFileHandler>
    <events name="AllAuthn" eventName="SECURITY_AUTHN" />
```

Remediation:

Modify the ${server.config.dir}/server.xml file and configure the audit-1.0 feature.

Configure the auditFileHandler setting to record SECURITY_AUTHN and SECURITY_AUTHZ events.

Review audit logs located under the ${server.config.dir}/logs directory and ensure AUTHN and AUTHZ events are logged.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-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)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	IBMW-LS-000010 (Manual)	☐	☐
1.2	IBMW-LS-000020 (Manual)	☐	☐
1.3	IBMW-LS-000030 (Manual)	☐	☐
1.4	IBMW-LS-000040 (Manual)	☐	☐
1.5	IBMW-LS-000050 (Manual)	☐	☐
1.6	IBMW-LS-000230 (Manual)	☐	☐
1.7	IBMW-LS-000260 (Manual)	☐	☐
1.8	IBMW-LS-000280 (Manual)	☐	☐
1.9	IBMW-LS-000320 (Manual)	☐	☐
1.10	IBMW-LS-000340 (Manual)	☐	☐
1.11	IBMW-LS-000370 (Manual)	☐	☐
1.12	IBMW-LS-000380 (Manual)	☐	☐
1.13	IBMW-LS-000381 (Manual)	☐	☐
1.14	IBMW-LS-000390 (Manual)	☐	☐
1.15	IBMW-LS-000440 (Manual)	☐	☐
1.16	IBMW-LS-000450 (Manual)	☐	☐
1.17	IBMW-LS-000500 (Manual)	☐	☐
1.18	IBMW-LS-000520 (Manual)	☐	☐
1.19	IBMW-LS-000720 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	IBMW-LS-000770 (Manual)	☐	☐
1.21	IBMW-LS-000790 (Manual)	☐	☐
1.22	IBMW-LS-000830 (Manual)	☐	☐
1.23	IBMW-LS-000910 (Manual)	☐	☐
1.24	IBMW-LS-000970 (Manual)	☐	☐
1.25	IBMW-LS-001050 (Manual)	☐	☐
1.26	IBMW-LS-001110 (Manual)	☐	☐
1.27	IBMW-LS-001120 (Manual)	☐	☐
1.28	IBMW-LS-001170 (Manual)	☐	☐
1.29	IBMW-LS-001190 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 26, 2025	1.0.0	Initial CIS Release