CIS Center for Internet Security

CIS Benchmarks™

CIS Apache Tomcat Application Server 9 Security Technical Implementation Guide STIG Benchmark

v1.0.0 - 09-11-2025

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

Apache Tomcat Application Server 9 Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)
Version: 3 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 Apache Tomcat Application Server 9 Security Technical Implementation Guide 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 Apache Tomcat Application Server 9 Security Technical Implementation Guide.

Recommendations

1 STIG RULES

Apache Tomcat Server 9

Apache Tomcat Application Server 9 Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)

Version: 3 Release: 2 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 TCAT-AS-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Secured connectors must be configured to use strong encryption ciphers.

```
GROUP ID: V-222927
RULE ID: SV-222927r960759
```

Rationale:

The Tomcat <Connector> element controls the TLS protocol and the associated ciphers used. If a strong cipher is not selected, an attacker may be able to circumvent encryption protections that are configured for the connector. Strong ciphers must be employed when configuring a secured connector.

The configuration attribute and its values depend on what HTTPS implementation the user is utilizing. The user may be utilizing either Java-based implementation aka JSSE — with BIO and NIO connectors, or OpenSSL-based implementation — with APR connector.

TLSv1.2 ciphers are configured via the server.xml file on a per connector basis. For a list of approved ciphers, refer to NIST SP 800-52 section 3.3.1.1.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i ciphers $CATALINA_BASE/conf/server.xml.
Examine each <Connector/> element that is not a redirect to a secure port. Identify the ciphers that are configured on each connector and determine if any of the ciphers are not secure.
For a list of approved ciphers, refer to NIST SP 800-52 section 3.3.1.1.
If insecure ciphers are configured for use, this is a finding.

Remediation:

As a privileged user on the Tomcat server, edit the $CATALINA_BASE/conf/server.xml and modify the <Connector/> element.
Add the SSLEnabledProtocols="TLSv1.2" setting to the connector or modify the existing setting.
Set SSLEnabledProtocols="TLSv1.2". Save the server.xml file and restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl reload-daemon

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)

1.2 TCAT-AS-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The number of allowed simultaneous sessions to the manager application must be limited.

```
GROUP ID: V-222926
RULE ID: SV-222926r960735
```

Rationale:

The manager application provides configuration access to the Tomcat server. Access to the manager application must be limited and that includes the number of sessions allowed to access the management application. A balance must be struck between the number of simultaneous connections allowed to the management application and the number of authorized admins requiring access at any given time.

Determine the number of authorized admins requiring simultaneous access and increase the number of allowed simultaneous sessions by a small percentage in order to help prevent potential lockouts.

Document that value in the System Security Plan (SSP).

Audit:

If the manager application is not in use or has been deleted from the system, this is not a finding.
From the Tomcat server as an elevated user run the following command:
sudo grep -i maxactivesessions $CATALINA_BASE/webapps/manager/ META-INF/context.xml
If the maxActiveSesions setting is not configured according to the number of connections defined in the SSP, this is a finding.

Remediation:

Determine the number of authorized admins requiring simultaneous access and increase the number of allowed simultaneous sessions by a small percentage in order to address potential lockout scenarios. Document that value in the System Security Plan.
Review the maxActiveSessions setting in the $CATALINA_BASE/webapps/manager/ META-INF/context.xml configuration file.
Configure maxActiveSessions setting according to admin access requirements defined in the SSP.
EXAMPLE:
<Manager … maxActiveSessions="10" />

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 TCAT-AS-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

HTTP Strict Transport Security (HSTS) must be enabled.

```
GROUP ID: V-222928
RULE ID: SV-222928r960762
```

Rationale:

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

Implementing HSTS requires testing of your web applications to ensure SSL certificates align correctly with application requirements and sub-domains if sub-domains are used. Ensure certificates are installed and working correctly. If sub-domains are in use, all sub-domains must be covered in the SSL/TLS certificate and the includeSubDomains directive must be specified in order for HSTS to function properly.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i -A5 -B8 hstsEnable $CATALINA_BASE/conf/web.xml file.
If the httpHeaderSecurity filter is commented out or if hstsEnable is not set to "true", this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the web.xml file:
sudo nano $CATALINA_BASE/conf/web.xml file.
Uncomment the existing httpHeaderSecurity filter section or create the filter section using the following code:
NOTE: includeSubDomains param-value and url-pattern values may change and can vary according to local deployment requirements.

httpHeaderSecurity
org.apache.catalina.filters.HttpHeaderSecurityFilter

hstsEnabled
true

hstsMaxAgeSeconds
31536000

hstsIncludeSubDomains
true

true

Create or uncomment the httpHeaderSecurity filter mapping:

httpHeaderSecurity
/*
REQUEST

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 TCAT-AS-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

TLS 1.2 must be used on secured HTTP connectors.

```
GROUP ID: V-222929
RULE ID: SV-222929r960762
```

Rationale:

Using older versions of TLS introduces security vulnerabilities that exist in the older versions of the protocol. Tomcat by default will use all available versions of the SSL/TLS protocols unless the version is explicitly defined in the SSL configuration attribute for the associated connector. This introduces the opportunity for the client to negotiate the use of an older protocol version and increases the risk of compromise of the Tomcat server.

All connectors must use TLS 1.2. While this check specifically verifies the use of TLSv1.2, it does not provide all of the steps required to successfully configure a secured TLS connection. That task involves multiple additional steps that are not included here. Refer to Tomcat documentation for all of the steps needed to create a TLS protected connector.

Satisfies: SRG-APP-000015-AS-000010, SRG-APP-000172-AS-000120, SRG-APP-000439-AS-000155

Audit:

From the Tomcat server console, run the following command:
sudo cat $CATALINA_BASE/conf/server.xml.
Examine each <Connector/> element.
For every HTTP protocol connector:
Verify the SSLEnabledProtocols="TLSv1.2" flag is set on each connector.
If the SSLEnabledProtocols setting is not set to TLSv1.2 or greater, this is a finding.

Remediation:

As a privileged user on the Tomcat server, edit the $CATALINA_BASE/conf/server.xml and modify the <Connector/> element.
Add the "SSLEnabledProtocols=" flag to the connector or modify the existing flag.
Set SSLEnabledProtocols="TLSv1.2". Save the server.xml file and restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl reload-daemon

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

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

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

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

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

1.5 TCAT-AS-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

AccessLogValve must be configured for each application context.

```
GROUP ID: V-222930
RULE ID: SV-222930r960765
```

Rationale:

Tomcat has the ability to host multiple contexts (applications) on one physical server by using the <Host><Context> attribute. This allows the admin to specify audit log settings on a per application basis.

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-000098-AS-000061, SRG-APP-000099-AS-000062

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review for all <Context> elements.
If a <Valve className="org.apache.catalina.valves.AccessLogValve" .../> element is not defined within each <Context> element, this is a finding.
EXAMPLE:
<Context
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="application_name_log" suffix=".txt"
pattern=""%h %l %t %u "%r" %s %b" />
...
/>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Create a <Valve> element that is nested within the <Context> element containing an AccessLogValve.
EXAMPLE:
<Context
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="application_name_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
/>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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-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-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

1.6 TCAT-AS-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Default password for keystore must be changed.

```
GROUP ID: V-222931
RULE ID: SV-222931r960792
```

Rationale:

Tomcat currently operates only on JKS, PKCS11, or PKCS12 format keystores. The JKS format is Java's standard "Java KeyStore" format, and is the format created by the keytool command-line utility which is included in the JDK. The PKCS12 format is an internet standard, and is managed using OpenSSL or Microsoft's Key-Manager. This requirement only applies to JKS keystores. When a new JKS keystore is created, if a password is not specified during creation the default password used by Tomcat is "changeit" (all lower case). If the default password is not changed, the keystore is at risk of compromise.

Satisfies: SRG-APP-000033-AS-000023, SRG-APP-000176-AS-000125

Audit:

From the Tomcat server console, run the following command to check the keystore:
sudo keytool -list -v
When prompted for the keystore password type "changeit" sans quotes.
If the contents of the keystore are displayed, this is a finding.

Remediation:

From the Tomcat server as a privileged user, run the following command:
sudo keytool -storepasswd
When prompted for the keystore password, select a strong password, minimum 10 characters, mixed case alpha-numeric.
Document the password and store in a secured location that is only accessible to authorized personnel.

Additional Information:

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

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

- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

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

1.7 TCAT-AS-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Cookies must have http-only flag set.

```
GROUP ID: V-222933
RULE ID: SV-222933r960792
```

Rationale:

It is possible to steal or manipulate web application session and cookies without having a secure cookie. Configuring the secure flag injects the setting into the response header.

The $CATALINA_BASE/conf/web.xml file controls how all applications handle cookies via the element.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i -B10 -A1 /cookie-config $CATALINA_BASE/conf/web.xml
If the command returns no results or if the element is not set to true, this is a finding.
EXAMPLE:

15

true
true

Remediation:

From the Tomcat server console as a privileged user:
edit the $CATALINA_BASE/conf/web.xml
If the cookie-config section does not exist it must be added. Add or modify the setting and set to true.
EXAMPLE:

15

true
true

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

1.8 TCAT-AS-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Cookies must have secure flag set.

```
GROUP ID: V-222932
RULE ID: SV-222932r960792
```

Rationale:

It is possible to steal or manipulate web application session and cookies without having a secure cookie. Configuring the secure flag injects the setting into the response header.

The $CATALINA_BASE/conf/web.xml file controls how all applications handle cookies via the element.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i -B10 -A1 /cookie-config $CATALINA_BASE/conf/web.xml
If the command returns no results or if the element is not set to true, this is a finding.
EXAMPLE:

15

true
true

Remediation:

From the Tomcat server console as a privileged user:
edit the $CATALINA_BASE/conf/web.xml
If the cookie-config section does not exist it must be added. Add or modify the setting and set to true.
EXAMPLE:

15

true
true

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

1.9 TCAT-AS-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DefaultServlet must be set to readonly for PUT and DELETE.

```
GROUP ID: V-222934
RULE ID: SV-222934r960792
```

Rationale:

The DefaultServlet is a servlet provided with Tomcat. It is called when no other suitable page can be displayed to the client. The DefaultServlet serves static resources as well as directory listings and is declared globally in $CATALINA_BASE/conf/web.xml. By default, Tomcat behaves as if the DefaultServlet is set to "true" (HTTP commands like PUT and DELETE are rejected). However, the readonly parameter is not in the web.xml file by default so to ensure proper configuration and system operation, the "readonly" parameter in web.xml must be created and set to "true". Creating the setting in web.xml provides assurances the system is operating as required. Changing the readonly parameter to false could allow clients to delete or modify static resources on the server and upload new resources.

Audit:

From the Tomcat server run the following command:
sudo cat $CATALINA_BASE/conf/web.xml |grep -i -A5 -B2 defaultservlet
If the "readonly" param-value for the "DefaultServlet" servlet class = "false" or does not exist, this is a finding.

Remediation:

From the Tomcat server console as a privileged user:
Edit the $CATALINA_BASE/conf/web.xml file.
If the "readonly" param-value does not exist, it must be created.
Ensure the "readonly" param-value for the "DefaultServlet" servlet class = "true".

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

1.10 TCAT-AS-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Connectors must be secured.

```
GROUP ID: V-222935
RULE ID: SV-222935r960792
```

Rationale:

The unencrypted HTTP protocol does not protect data from interception or alteration which can subject users to eavesdropping, tracking, and the modification of received data. To secure an HTTP connector, both the secure and scheme flags must be set.

Audit:

From the Tomcat server console, run the following command:
sudo cat $CATALINA_BASE/conf/server.xml.
Examine each <Connector/> element.
For each connector, verify the secure= flag is set to "true" and the scheme= flag is set to "https" on each connector.
If the secure flag is not set to "true" and/or the scheme flag is not set to "https" for each HTTP connector element, this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the server.xml file.
sudo nano $CATALINA_BASE/conf/server.xml.
Locate each <Connector/> element which is lacking a secure setting.
EXAMPLE Connector:
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="443" />
Set or add scheme="https" and secure="true" for each HTTP connector element.
EXAMPLE:
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
SSLEnabled="true"
maxThreads="150" scheme="https" secure="true".../>
Save the server.xml file and restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl reload-daemon

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

1.11 TCAT-AS-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Java Security Manager must be enabled.

```
GROUP ID: V-222936
RULE ID: SV-222936r1067546
```

Rationale:

The Java Security Manager (JSM) is what protects the Tomcat server from trojan servlets, JSPs, JSP beans, tag libraries, or even from inadvertent mistakes. The JSM works the same way a client's web browser isolates a running web application via a sandbox, the difference being the sandbox is running on the server rather than the client. To ensure application operability, JSM security policies must be set to allow the hosted application access to the underlying system based on individual application requirements. The JSM settings cannot be determined at the STIG level and will vary based on each hosted application.

Examples include setting JSM policy to allow an application to write to folders on the server or to initiate network connections to other servers via TCP/IP.

Because the JSM isolates application code to prevent an application from adversely accessing resources on the underlying Tomcat server, care must be taken to ensure the JSM policies are configured properly. Allowing untrusted web applications to run on the Tomcat server without a JSM policy that limits access to server resources creates a risk of compromise to the server.

Ideally, the JSM policy is implemented and tested during the application development phase. This is when the application resource requirements are best identified and documented so the correct JSM policy can be implemented in the production environment.

Creating the correct JSM policy can be a challenge when installing commercial software that does not provide the policy as part of the installation process or via documentation. This is due to the fact that the critical application access requirements to the system will typically not be known to the system administrator. In these cases, running the JSM can result in failure for some application functionality (e.g., an application might not be able to write logs to a particular folder on the system or communicate with other systems as intended).

When faced with application functionality failures, the typical troubleshooting approach for the system administrator to follow is to install the application in a test environment, set the $CATALINA_POLICY setting to debug, and identify failure events in the logs. This can aid in identifying what privileges the application requires. From there the JSM policies can be set, tested, documented, and transferred to production. If these actions do not address all of the issues, the Risk Management Framework processes come into effect and a risk acceptance for this requirement must be obtained from the ISSO.

For additional technical information on the security manager and available JSM policy settings, refer to the Security Manager How-To on the Apache Tomcat version 9 website.

Audit:

Review system documentation. Identify the tomcat systemd startup file, which for STIG purposes is called "tomcat.service" and can be viewed as a link in the /etc/systemd/system/ folder.
Run the following command:
sudo cat /etc/systemd/system/tomcat.service |grep -i security
If there is a documented and approved risk acceptance for not operating the Security Manager, this requirement is Not Applicable.
If the ExecStart parameter does not include the -security flag, this is a finding.

Remediation:

Refer to the vulnerability discussion of this requirement for additional information. Install the application in a test environment and determine the application access requirements. Test and document the Java Security Manager policy and then transfer the JSM policy to the $CATALINA_BASE/conf/catalina.properties file. If operating multiple instances of Tomcat, use $CATALINA_BASE in place of $CATALINA_HOME as per standard Tomcat practice.
As an admin user on the Tomcat server, modify the /etc/systemd/system/tomcat.service file and set the "ExecStart" parameter to read:

```
"ExecStart=/opt/tomcat/bin/startup.sh -security"
```

sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.12 TCAT-AS-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat servers behind a proxy or load balancer must log client IP.

```
GROUP ID: V-222937
RULE ID: SV-222937r960879
```

Rationale:

When running Tomcat behind a load balancer or proxy, default behavior is for Tomcat to log the proxy or load balancer IP address as the client IP. Desired behavior is to log the actual client IP rather than the proxy IP address. The RemoteIpValve logging component instructs Tomcat to grab the HTTP header X-Forwarded-For and use that for access logging.

Tomcat will identify 127.0.0.1, class A and class C RFC1918 addresses as internal proxy addresses; however, if the proxy has a routable IP or a class B private network address space (172.16.0.0/12), the user must also verify the "internalProxies setting is configured to reflect the proxy IP address.

Audit:

Review the System Security Plan and determine if the Tomcat server resides behind a proxy server or load balancer. If the Tomcat server is not behind a proxy server or load balancer, this requirement is NA.
From the Tomcat server run the following command:
sudo grep -i RemoteIpValve $CATALINA_BASE/conf/server.xml file.
If the results are empty or if the requestAttributesEnabled setting is not configured as "True", this is a finding.
sudo grep -i AccessLogValve $CATALINA_BASE/conf/server.xml file.
If the requestAttributesEnabled setting is not configured as "True", this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Edit the $CATALINA_BASE/conf/server.xml file.
Only execute this first step if the proxy server is using a routable IP address or an RFC 1918 Class B address space: Add or edit the RemoteIpValve and configure the internalProxies setting to reflect the proxy addresses.
Modify the AccessLogValve and configure the requestAttributesEnabled setting = "True".
EXAMPLE:

<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
prefix="access"
suffix=".log"
pattern="combined"
renameOnRotate="true"
requestAttributesEnabled="true"
/>
Restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl tomcat daemon-reload

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

1.13 TCAT-AS-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

AccessLogValve must be configured per each virtual host.

```
GROUP ID: V-222938
RULE ID: SV-222938r960882
```

Rationale:

Application servers utilize role-based access controls in order to specify the individuals who are allowed to configure application component loggable events. The application server must be configured to select which personnel are assigned the role of selecting which loggable events are to be logged.

Satisfies: SRG-APP-000090-AS-000051, SRG-APP-000095-AS-000056, SRG-APP-000100-AS-000063, SRG-APP-000101-AS-000072, SRG-APP-000503-AS-000228, SRG-APP-000505-AS-000230, SRG-APP-000506-AS-000231

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review for all <Host> elements.
If a <Valve className="org.apache.catalina.valves.AccessLogValve" .../> element is not nested within each <Host> element, this is a finding.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Create a <Valve> element that is nested beneath the <Host> element containing an AccessLogValve.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

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

CCI-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-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

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-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

1.14 TCAT-AS-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Date and time of events must be logged.

```
GROUP ID: V-222939
RULE ID: SV-222939r960894
```

Rationale:

The access logfile format is defined within a Valve that implements the org.apache.catalina.valves.AccessLogValve interface within the /opt/tomcat/server.xml configuration file: The %t pattern code is included in the pattern element and logs the date and time of the event. Including the date pattern in the log configuration provides useful information about the time of the event which is critical for troubleshooting and forensic investigations.

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review all "Valve" elements.
If the pattern= statement does not include %t, this is a finding.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Modify the <Valve> element(s) nested within the <Host> element(s).
Change the AccessLogValve setting to include %t in the pattern= statement.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

1.15 TCAT-AS-000250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Remote hostname must be logged.

```
GROUP ID: V-222940
RULE ID: SV-222940r960897
```

Rationale:

The access logfile format is defined within a Valve that implements the org.apache.catalina.valves.AccessLogValve interface within the /opt/tomcat/server.xml configuration file: The %h pattern code is included in the pattern element and logs the remote hostname. Including the hostname pattern in the log configuration provides useful information about the connecting host that is critical for troubleshooting and forensic investigations.

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review all "Valve" elements.
If the pattern= statement does not include %h, this is a finding.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Modify the <Valve> element(s) nested within the <Host> element(s).
Change the AccessLogValve setting to include %h in the pattern= statement.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

1.16 TCAT-AS-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

HTTP status code must be logged.

```
GROUP ID: V-222941
RULE ID: SV-222941r960897
```

Rationale:

The access logfile format is defined within a Valve that implements the org.apache.catalina.valves.AccessLogValve interface within the /opt/tomcat/server.xml configuration file: The %s pattern code is included in the pattern element and logs the server response code associated with the event e.g. 200 OK or 400 Bad Request. Including the status pattern in the log configuration provides useful server response information about the event which is critical for troubleshooting and forensic investigations.

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review all "Valve" elements.
If the pattern= statement does not include %s, this is a finding.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Modify the <Valve> element(s) nested within the <Host> element(s).
Change the AccessLogValve setting to include %s in the pattern= statement.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

1.17 TCAT-AS-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The first line of request must be logged.

```
GROUP ID: V-222942
RULE ID: SV-222942r960897
```

Rationale:

The access logfile format is defined within a Valve that implements the org.apache.catalina.valves.AccessLogValve interface within the /opt/tomcat/server.xml configuration file: The "%r" pattern code is included in the pattern element and logs the first line associated with the event, namely the request method, URL path, query string, and protocol (""" simply specifies a literal double quote). Including the pattern in the log configuration provides useful information about the time of the event which is critical for troubleshooting and forensic investigations.

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review all "Valve" elements.
If the pattern= statement does not include "%r", this is a finding.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Modify the <Valve> element(s) nested within the <Host> element(s).
Change the AccessLogValve setting to include "%r" in the pattern= statement.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

1.18 TCAT-AS-000360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_BASE/logs folder permissions must be set to 750.

```
GROUP ID: V-222943
RULE ID: SV-222943r960930
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/logs -follow -maxdepth 0 -type d (! -perm 750) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/logs folder permissions are not set to 750, this is a finding.

Remediation:

If operational/application requirements specify different file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following command on the Tomcat server:
sudo find $CATALINA_BASE/logs -follow -maxdepth 0 -type d -print0 | sudo xargs chmod 750 $CATALINA_BASE/logs

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

1.19 TCAT-AS-000361 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files in the $CATALINA_BASE/logs/ folder must have their permissions set to 640.

```
GROUP ID: V-222944
RULE ID: SV-222944r960930
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/logs/* -follow -maxdepth 0 -type f (! -perm 640) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no files are displayed, this is not a finding.
If results indicate any of the file permissions contained in the $CATALINA_BASE/logs folder are not set to 640, this is a finding.

Remediation:

If operational/application requirements specify different file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following command on the Tomcat server:
sudo find $CATALINA_BASE/logs/* -follow -maxdepth 0 -type f -print0 | sudo xargs chmod 640 $CATALINA_BASE/logs/*

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

1.20 TCAT-AS-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files in the $CATALINA_BASE/conf/ folder must have their permissions set to 640.

```
GROUP ID: V-222945
RULE ID: SV-222945r960933
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user group tomcat rather than root user group tomcat. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

If the ISSM determines the operational need to allow application admins access to change the Tomcat configuration outweighs the risk of limiting that access, then they can change the group membership to accommodate. Ownership must not be changed. The ISSM should take the exposure of the system to high risk networks into account.

Satisfies: SRG-APP-000119-AS-000079, SRG-APP-000380-AS-000088

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/conf/* -follow -maxdepth 0 -type f (! -perm 640) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no files are displayed, this is not a finding.
If results indicate any of the file permissions contained in the $CATALINA_BASE/conf folder are not set to 640, this is a finding.

Remediation:

If operational/application requirements specify different file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following command on the Tomcat server:
sudo find $CATALINA_BASE/conf/* -follow -maxdepth 0 -type f -print0 | sudo xargs chmod 640 $CATALINA_BASE/conf/*

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-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)

1.21 TCAT-AS-000371 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_BASE/conf folder permissions must be set to 750.

```
GROUP ID: V-222946
RULE ID: SV-222946r960933
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

If the ISSM determines the operational need to allow application admins access to change the Tomcat configuration outweighs the risk of limiting that access, then they can change the group membership to accommodate. Ownership must not be changed. The ISSM should take the exposure of the system to high risk networks into account.

Satisfies: SRG-APP-000119-AS-000079, SRG-APP-000380-AS-000088

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/conf -follow -maxdepth 0 -type d (! -perm 750) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/conf folder permissions are not set to 750, this is a finding.

Remediation:

If operational/application requirements specify different file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following command on the Tomcat server:
sudo find $CATALINA_BASE/conf -follow -maxdepth 0 -type d -print0 | sudo xargs chmod 750 $CATALINA_BASE/conf

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-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)

1.22 TCAT-AS-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Jar files in the $CATALINA_HOME/bin/ folder must have their permissions set to 640.

```
GROUP ID: V-222947
RULE ID: SV-222947r960936
```

Rationale:

Tomcat's file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with the group Tomcat. While root has read/write privileges, tomcat group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_HOME/bin/*jar -follow -maxdepth 0 -type f (! -perm 640) -ls
If there are no results, or if .sh extensions are found, this is not a finding.
If results indicate any of the jar file permissions contained in the $CATALINA_HOME/bin folder are not set to 640, this is a finding.

Remediation:

Run the following command on the Tomcat server:
sudo find $CATALINA_HOME/bin/*jar -follow -maxdepth 0 -type f -print0 | sudo xargs chmod 640 $CATALINA_HOME/bin/*jar

Additional Information:

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

1.23 TCAT-AS-000390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_HOME/bin folder permissions must be set to 750.

```
GROUP ID: V-222948
RULE ID: SV-222948r960939
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions. Note that running Tomcat in a Docker environment can impact how file permissions and user ownership settings are applied. Due to associated Docker configuration complexities, the STIG is scoped for standalone rather than virtual Docker deployments.

Satisfies: SRG-APP-000121-AS-000081, SRG-APP-000122-AS-000082, SRG-APP-000123-AS-000083, SRG-APP-000340-AS-000185

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_HOME/bin -follow -maxdepth 0 -type d (! -perm 750) -ls
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_HOME/bin folder permissions are not set to 750, this is a finding.

Remediation:

Run the following command on the Tomcat server:
sudo find $CATALINA_HOME/bin -follow -maxdepth 0 -type d -print0 | sudo xargs chmod 750 $CATALINA_HOME/bin

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

CCI-001494 Protect audit tools 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-001495 Protect audit tools 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

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)

1.24 TCAT-AS-000450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat user UMASK must be set to 0027.

```
GROUP ID: V-222949
RULE ID: SV-222949r960960
```

Rationale:

For Unix-based systems, umask settings affect file creation permissions. If the permissions are too loose, newly created log files and applications could be accessible to unauthorized users via the file system. Ensure the Tomcat OS user account has the correct file creation permission settings by validating the OS umask settings for the Tomcat user. Setting umask to 0027 gives the Tomcat user full rights, group users r-x permission and all others no access. Tomcat will most likely be running as a systemd service. Locate the systemd service file for Tomcat. The default location for the link to the service file is in /etc/systemd/system folder. The service file name should be indicative of the Tomcat process so tomcat.service is the logical name for the service file and is the name referenced by the STIG.

Audit:

Reference the system documentation and make relevant changes to the following commands if the system differs:
From the Tomcat server command line run the following command:
sudo cat /etc/systemd/system/tomcat.service | grep -i umask
If the umask is not = 0027, this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Use a file editor like nano or vi and edit the /etc/systemd/system/tomcat.service file.
Change the "UMask=" setting to 0027.
UMask =0027
Save the file and restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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)

1.25 TCAT-AS-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Stack tracing must be disabled.

```
GROUP ID: V-222950
RULE ID: SV-222950r960963
```

Rationale:

Stack tracing provides debugging information from the application call stacks when a runtime error is encountered. If stack tracing is left enabled, Tomcat will provide this call stack information to the requestor which could result in the loss of sensitive information or data that could be used to compromise the system. As with all STIG settings, it is acceptable to temporarily enable for troubleshooting and debugging purposes but the setting must not be left enabled after troubleshooting tasks have been completed.

Audit:

From the Tomcat server run the following OS command:
sudo cat $CATALINA_BASE/conf/server.xml | grep -i connector
Review each connector element, ensure each connector does not have an "allowTrace" setting or ensure the "allowTrace" setting is set to false.
<Connector ... allowTrace="false" />
Do the same for each application by checking every $CATALINA_BASE/webapps/<APP_NAME>/WEBINF/web.xml file on the system.
sudo cat $CATALINA_BASE/webapps/<APP_NAME>/WEBINF/web.xml |grep -i connector
If a connector element in the server.xml file or in any of the <APP NAME>/WEBINF/web.xml files contains the "allow Trace = true" statement, this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the xml files containing the "allow Trace=true" statement.
Remove the "allow Trace=true" statement from the affected xml configuration files and restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.26 TCAT-AS-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The shutdown port must be disabled.

```
GROUP ID: V-222951
RULE ID: SV-222951r960963
```

Rationale:

Tomcat listens on TCP port 8005 to accept shutdown requests. By connecting to this port and sending the SHUTDOWN command, all applications within Tomcat are halted. The shutdown port is not exposed to the network as it is bound to the loopback interface. Set the shutdown attribute in $CATALINA_BASE/conf/server.xml.

Audit:

From the Tomcat server run the following OS command:

```
$ sudo grep -i shutdown $CATALINA_BASE/conf/server.xml
```

Ensure the server shutdown port attribute in $CATALINA_BASE/conf/server.xml is set to -1.
EXAMPLE:
<Server port="-1" shutdown="SHUTDOWN">
If Server port not = "-1" shutdown="SHUTDOWN", this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the $CATALINA_BASE/conf/server.xml file: set the Server port setting to -1 and restart the Tomcat server.

sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.27 TCAT-AS-000500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unapproved connectors must be disabled.

```
GROUP ID: V-222952
RULE ID: SV-222952r960963
```

Rationale:

Connectors are how Tomcat receives requests, passes them to hosted web applications, and then sends back the results to the requestor. Tomcat provides HTTP and Apache JServ Protocol (AJP) connectors and makes these protocols available via configured network ports. Unapproved connectors provide open network connections to either of these protocols and put the system at risk.

Audit:

Review SSP for list of approved connectors and associated TCP/IP ports. Ensure only approved connectors are present. Execute the following command on the Tomcat server to find configured Connectors:

```
$ grep "Connector" $CATALINA_BASE/conf/server.xml
```

Review results and verify all connectors and their associated network ports are approved in the SSP.
If connectors are found but are not approved in the SSP, this is a finding.

Remediation:

Obtain ISSO approvals for the configured connectors and document in the SSP.
Alternatively, edit the $CATALINA_BASE/conf/server.xml file, remove any unapproved connectors, and restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.28 TCAT-AS-000510 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

DefaultServlet debug parameter must be disabled.

```
GROUP ID: V-222953
RULE ID: SV-222953r960963
```

Rationale:

The DefaultServlet serves static resources as well as serves the directory listings (if directory listings are enabled). It is declared globally in $CATALINA_BASE/conf/web.xml and by default is configured with the "debug" parameter set to 0, which is disabled. Changing this to a value of 1 or higher sets the servlet to print debug level information. DefaultServlet debug setting must be set to 0 (disabled).

Audit:

From the Tomcat server run the following OS command:
sudo cat $CATALINA_BASE/conf/web.xml |grep -i -A10 -B2 defaultservlet
The above command will include ten lines after and two lines before the occurrence of "defaultservlet". Some systems may require that the user increase the after number (A10) in order to determine the "debug" param-value.
If the "debug" param-value for the "DefaultServlet" servlet class does not = 0, this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Edit the $CATALINA_BASE/conf/web.xml file.
Examine the elements within the <Servletclass> element, if the "debug" element is not "0"" change the "debug" to read "0".
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.29 TCAT-AS-000520 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

DefaultServlet directory listings parameter must be disabled.

```
GROUP ID: V-222954
RULE ID: SV-222954r960963
```

Rationale:

The DefaultServlet serves static resources as well as directory listings. It is declared globally in $CATALINA_BASE/conf/web.xml and by default is configured with the directory "listings" parameter set to disabled. If no welcome file is present and the "listings" setting is enabled, a directory listing is shown. Directory listings must be disabled.

Audit:

From the Tomcat server run the following OS command:
sudo cat $CATALINA_BASE/conf/web.xml |grep -i -A10 -B2 defaultservlet
The above command will include ten lines after and two lines before the occurrence of "defaultservlet". Some systems may require that the user increase the after number (A10) in order to determine the "listings" param-value.
If the "listings" param-value for the "DefaultServlet" servlet class does not = "false", this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Edit the $CATALINA_BASE/conf/web.xml file.
Examine the elements within the <Servletclass> element, if the "listings" element is "true" change the "listings" to read "false".
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.30 TCAT-AS-000530 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The deployXML attribute must be set to false in hosted environments.

```
GROUP ID: V-222955
RULE ID: SV-222955r960963
```

Rationale:

The Host element controls deployment. Automatic deployment allows for simpler management, but also makes it easier for an attacker to deploy a malicious application. Automatic deployment is controlled by the autoDeploy and deployOnStartup attributes. If both are false, only Contexts defined in server.xml will be deployed, and any changes will require a Tomcat restart.

In a hosted environment where web applications may not be trusted, set the deployXML attribute to false to ignore any context.xml packaged with the web application that may try to assign increased privileges to the web application. Note that if the security manager is enabled that the deployXML attribute will default to false.

This requirement is NA for test and development systems on non-production networks. For DevSecOps application environments, the ISSM may authorize autodeploy functions on a production Tomcat system if the mission need specifies it and an application security vulnerability testing and assurance regimen is included in the DevSecOps process.

Audit:

If the SSP associated with the Host contains ISSM documented approvals for deployXML, this is not a finding.
From the Tomcat server as a privileged user:
sudo grep -i deployXML $CATALINA_BASE/conf/server.xml
deployXML="false"
If the deployXML="true" and there is no documented authorization to allow automatic deployment of applications, this is a finding.
If no results are generated, confirm the default behavior is "false". For example: If the attribute is not set and security manager is not enabled, the default value is "true". When security manager is enabled, the default value is "false".
If the default value is "true", this is a finding.

Remediation:

Document authorization for application auto deployment in the System Security Plan (SSP).
From the Tomcat server as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
sudo nano $CATALINA_BASE/conf/server.xml
Locate each element in the server xml file.
If the deployXML="true" ensure each host is authorized for application auto deployment and document the authorization in the system security plan.
If authorization is not provided, set the deployXML="false".

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

1.31 TCAT-AS-000540 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Autodeploy must be disabled.

```
GROUP ID: V-222956
RULE ID: SV-222956r960963
```

Rationale:

Tomcat allows auto-deployment of applications while Tomcat is running. This can allow untested or malicious applications to be automatically loaded into production. Autodeploy must be disabled in production.

This requirement is NA for test and development systems on non-production networks. For DevSecOps application environments, the ISSM may authorize autodeploy functions on a production Tomcat system if the mission need specifies it and an application security vulnerability testing and assurance regimen is included in the DevSecOps process.

Audit:

If the SSP associated with the Host contains ISSM-documented approvals for AutoDeploy, this is not a finding.
From the Tomcat server, run the following OS command:
sudo cat $CATALINA_BASE/conf/server.xml | grep -i -C2 autodeploy
If the command returns no results, this is not a finding.
Review the results for the autoDeploy parameter in each Host element.

If autoDeploy ="true" or if autoDeploy is not set, this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
Examine each <Host> </Host> element, if the element contains autoDeploy="true", modify the statement to read ", autoDeploy="false".
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.32 TCAT-AS-000550 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

xpoweredBy attribute must be disabled.

```
GROUP ID: V-222957
RULE ID: SV-222957r960963
```

Rationale:

Individual connectors can be configured to display the Tomcat server info to clients. This information can be used to identify Tomcat versions which can be useful to attackers for identifying vulnerable versions of Tomcat. Individual connectors must be checked for the xpoweredBy attribute to ensure they do not pass Tomcat server info to clients.

Audit:

From the Tomcat server run the following OS command:
sudo cat $CATALINA_BASE/conf/server.xml |grep -i -C4 xpoweredby.
If any connector elements contain xpoweredBy="true", this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
Examine each <Connector> </Connector> element, if the element contains xpoweredBy="true", modify the statement to read ", xpoweredBy="false".
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.33 TCAT-AS-000560 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Example applications must be removed.

```
GROUP ID: V-222958
RULE ID: SV-222958r960963
```

Rationale:

Tomcat provides example applications, documentation, and other directories in the default installation which do not serve a production use. These files must be deleted.

Audit:

From the Tomcat server OS type the following command:
sudo ls -l $CATALINA_BASE/webapps/examples.
If the examples folder exists or contains any content, this is a finding.

Remediation:

From the Tomcat server OS type the following command:
sudo rm -rf $CATALINA_BASE/webapps/examples

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

1.34 TCAT-AS-000570 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Tomcat default ROOT web application must be removed.

```
GROUP ID: V-222959
RULE ID: SV-222959r960963
```

Rationale:

The default ROOT web application includes the version of Tomcat that is being used, links to Tomcat documentation, examples, FAQs, and mailing lists. The default ROOT web application must be removed from a publicly accessible Tomcat instance and a more appropriate default page shown to users. It is acceptable to replace the contents of default ROOT with a new default web application.

WARNING: Removing the ROOT folder without replacing the content with valid web based content will result in an error page being displayed to the browser when the browser lands on the default page.

Audit:

From the Tomcat server OS type the following command:
sudo ls -l $CATALINA_BASE/webapps/ROOT
Review the index.jsp file. Also review the RELEASE-NOTES.txt file. Look for content that describes the application as being licensed by the Apache Software Foundation. Check the index.jsp for other verbiage that indicates the application is part of the Tomcat server. Alternatively, use a web browser and access the default web application and determine if the website application in the ROOT folder is provided with the Apache Tomcat server.
If the ROOT web application contains Tomcat default application content, this is a finding.

Remediation:

WARNING: Removing the ROOT folder without replacing the content with valid web based content will result in an error page being displayed to the browser when the browser lands on the default page.
From the Tomcat server OS:
Either remove the files contained in $CATALINA_BASE/webapps/ROOT folder or replace the content of the folder with a new application that serves as the new default server application.

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

1.35 TCAT-AS-000580 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Documentation must be removed.

```
GROUP ID: V-222960
RULE ID: SV-222960r960963
```

Rationale:

Tomcat provides documentation and other directories in the default installation which do not serve a production use. These files must be deleted.

Audit:

From the Tomcat server OS type the following command:
sudo ls -l $CATALINA_BASE/webapps/docs.
If the docs folder exists or contains any content, this is a finding.

Remediation:

From the Tomcat server OS type the following command:
sudo rm -rf $CATALINA_BASE/webapps/docs

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

1.36 TCAT-AS-000590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Applications in privileged mode must be approved by the ISSO.

```
GROUP ID: V-222961
RULE ID: SV-222961r1043177
```

Rationale:

The privileged attribute controls if a context (application) is allowed to use container provided servlets like the Manager servlet. It is false by default and should only be changed for trusted web applications.

Set to true to allow the context (application) to use container servlets, like the manager servlet. Use of the privileged attribute will change the context's parent class loader to be the Server class loader rather than the Shared class loader. Note that in a default installation, the Common class loader is used for both the Server and the Shared class loaders. Use of the privileged attribute will change the context's parent class loader to be the Server class loader rather than the Shared class loader.

Audit:

Individual Context elements may be explicitly defined in an individual file located at /META-INF/context.xml inside the application files or in the $CATALINA_BASE/conf/context.xml file. It is not recommended to store the context element in the server.xml file as changes will require a server restart.
The $CATALINA_BASE/conf/context element information will be loaded by all web applications, the META-INF/context.xml will only be loaded by that specific application.
On the Tomcat server as a privileged user run the following commands:
grep -i privileged $CATALINA_BASE/conf/context.xml
Repeat the following command for each installed application:
grep -i privileged $CATALINA_BASE/webapps/META-INF/context.xml
If the privileged context attribute is set to true, confirm the application has been approved for privileged mode by the ISSO. If the application is not approved to run in privileged mode, this is a finding.

Remediation:

On the Tomcat server as a privileged user, modify the relevant context.xml file and set the privileged attribute to false (privileged=false).
A restart should not be required if the context element is not maintained in the server.xml file.
If privileged mode is required for a particular application, verify trust of application and obtain documented approval from the ISSO. Document the applications that are approved to run in privileged mode and retain approvals in the system security plan (SSP) for CCRI reviews.

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

1.37 TCAT-AS-000600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat management applications must use LDAP realm authentication.

```
GROUP ID: V-222962
RULE ID: SV-222962r1051118
```

Rationale:

Using the local user store on a Tomcat installation does not meet a multitude of security control requirements related to user account management. To address this risk, Tomcat must be configured to utilize an LDAP or Active Directory installation that provides a centralized user account store that is configured to meet standard DoD user account management requirements. JNDIRealm is an implementation of the Tomcat Realm interface that looks up users in an LDAP directory server accessed by a JNDI provider (typically, the standard LDAP provider that is available with the JNDI API classes). The realm supports a variety of approaches to using a directory for authentication.

Audit:

If manager and host-manager applications have been deleted from the system, this is not a finding.
From the Tomcat server as a privileged user, run the following commands:
sudo grep -i -A8 JNDIRealm $CATALINA_BASE/conf/server.xml
If the JNDIRealm does not exist or if the JNDIRealm configuration is commented out, this is finding.

Remediation:

Identify the server IP that is providing LDAP services and configure the Tomcat user roles schema within LDAP. Refer to the manager and host-manager web.xml files for application specific role information that can be used for setting up the roles for those applications. The default location for these files is:
$CATALINA_BASE/webapps/<AppName>/WEB-INF/web.xml
From the Tomcat server console as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
Locate the <Realm> element in the server.xml file, add a nested <Realm> element using the JNDIRealm className and configure the associated LDAP settings as per the LDAP server connection requirements.
EXAMPLE:
This is for illustration purposes only. Modify the LDAP settings on a case-by-case basis as per the individual LDAP server and schema.
<Realm className="org.apache.catalina.realm.JNDIRealm"
connectionURL="ldaps://localhost:686"
userPattern="uid={0},ou=people,dc=myunit,dc=mil"
roleBase="ou=groups,dc=myunit,dc=mil"
roleName="cn"
roleSearch="(uniqueMember={0})"
/>

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

1.38 TCAT-AS-000610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

JMX authentication must be secured.

```
GROUP ID: V-222963
RULE ID: SV-222963r960972
```

Rationale:

Java Management Extensions (JMX) provides the means to remotely manage the Java VM. When enabling the JMX agent for remote monitoring, the user must enable authentication.

Audit:

From the Tomcat server run the following command:
sudo grep -I jmxremote.authenticate /etc/systemd/system/tomcat.service
sudo ps -ef |grep -i jmxremote
If the results are blank, this is not a finding.
If the results include:
-Dcom.sun.management.jmxremote.authenticate=false, this is a finding.

Remediation:

If using JMX for management of the Tomcat server, start the Tomcat server by adding the following command line flags to the systemd startup scripts in /etc/systemd/system/tomcat.service.
Environment='CATALINA_OPTS -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.ssl=true'
sudo systemctl start tomcat
sudo systemctl daemon-reload

Additional Information:

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)

1.39 TCAT-AS-000630 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

TLS must be enabled on JMX.

```
GROUP ID: V-222964
RULE ID: SV-222964r1016511
```

Rationale:

Java Management Extensions (JMX) provides the means for enterprises to remotely manage the Java VM and can be used in place of the local manager application that comes with Tomcat.

JMX management is configured via the Tomcat CATALINA_OPTS setting maintained in the /etc/systemd/system/tomcat.service file for Ubuntu systemd Unix. For Linux OS flavors other than Ubuntu, use the relevant OS commands.

Management tasks such as monitoring and control of applications is accomplished via the jmxremote servlet. If authentication is disabled, an attacker only needs to know the port number in order to manage and control hosted Java applications.

Audit:

JMX management is configured via the Tomcat CATALINA_OPTS environment variable setting maintained in the /etc/systemd/system/tomcat.service file for Ubuntu systemd UNIX. For other flavors of Linux, this location may vary.
As a privileged user from the Tomcat server, run the following command:
grep -i jmxremote /etc/systemd/system/tomcat.service
Review the output. If there are no results displayed, or jmxremote management extensions are not used, this requirement is Not Applicable.
If the JMXremote setting is configured and jmxremote.ssl="false", this is a finding.
EXAMPLE:
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false

Remediation:

If using JMX for management of the Tomcat server, start the Tomcat server by adding the following command line flags to the systemd startup scripts in /etc/systemd/system/tomcat.service.
Environment='CATALINA_OPTS -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.authenticate=true -Dcom.sun.management.jmxremote.ssl=true'
sudo systemctl start tomcat
sudo systemctl daemon-reload

Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

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

1.40 TCAT-AS-000690 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

LDAP authentication must be secured.

```
GROUP ID: V-222965
RULE ID: SV-222965r961029
```

Rationale:

JNDIRealm is an implementation of the Tomcat Realm interface. Tomcat uses the JNDIRealm to look up users in an LDAP directory server. The realm's connection to the directory is defined by the 'connectionURL' configuration attribute. This attribute is usually an LDAP URL that specifies the domain name of the directory server to connect to.

The LDAP URL does not provide encryption by default. This can lead to authentication credentials being transmitted across network connections in clear text.

To address this risk, Tomcat must be configured to use secure LDAP (LDAPS).

Audit:

From the Tomcat server as a privileged user, run the following commands:
sudo grep -i -A8 JNDIRealm $CATALINA_BASE/conf/server.xml
If the JNDIRealm connectionURL setting is not configured to use LDAPS, if it does not exist, or is commented out, this is a finding.
EXAMPLE:
This is an example. Substitute localhost for the LDAP server IP and configure other LDAP-related settings as well.
<Realm className="org.apache.catalina.realm.JNDIRealm"
connectionURL="ldaps://localhost:686"
...
/>

Remediation:

Identify the server IP that is providing LDAP services and configure the Tomcat user roles schema within LDAP. Refer to the manager and host-manager web.xml files for application specific role information that can be used for setting up the roles for those applications. The default location for these files is:
$CATALINA_BASE/webapps/<AppName>/WEB-INF/web.xml
From the Tomcat server console as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
Locate the <Realm> element in the server.xml file, add a nested <Realm> element using the JNDIRealm className and configure the associated LDAP settings as per the LDAP server connection requirements.
EXAMPLE:
This is for illustration purposes only. The user must modify the LDAP settings on a case by case basis as per your individual LDAP server and schema.
<Realm className="org.apache.catalina.realm.JNDIRealm"
connectionURL="ldaps://localhost:686"
userPattern="uid={0},ou=people,dc=myunit,dc=mil"
roleBase="ou=groups,dc=myunit,dc=mil"
roleName="cn"
roleSearch="(uniqueMember={0})"
/>

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)

1.41 TCAT-AS-000700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

DOD root CA certificates must be installed in Tomcat trust store.

```
GROUP ID: V-222966
RULE ID: SV-222966r985891
```

Rationale:

Tomcat truststores are used to validate client certificates. On the Ubuntu OS, by default, Tomcat uses the "cacerts" file as the CA trust store. The file is located in the /etc/ssl/certs/java/ folder with a link to the file in $JAVA_HOME/lib/security/cacerts. However, this location can be modified by setting the value of the javax.net.ssl.trustStore system property. Setting this property within an OS environment variable will change the location to point to a different trust store.

The Java OS environment variables in the systemd Tomcat startup file must be checked in order to identify the location of the trust store on the file system. (The STIG uses the name tomcat.service as a reference, but technically this file can be called anything).

If the property is not set, then the default location is used for the truststore.

Audit:

This is a mutual authentication requirement where both the Tomcat server and the client are required to authenticate themselves via mutual TLS. Review system security plan and other system documentation. If the system has no connections requiring mutual authentication (e.g., proxy servers or other hosts specified in the system documentation), this requirement is Not Applicable.
For the systemd Ubuntu OS, check the tomcat.service file to read the content of the JAVA_OPTS environment variable setting.
sudo cat /etc/systemd/system/tomcat.service |grep -i truststore
EXAMPLE output:
set JAVA_OPTS="-Djavax.net.ssl.trustStore=/path/to/truststore" "-Djavax.net.ssl.trustStorePassword=**********"
If the variable is not set, use the default location command below. If the variable is set, use the alternate location command below and include the path and truststore file.
-Default location:
keytool -list -cacerts -v | grep -i issuer
-Alternate location:
keytool -list -keystore -v |grep -i issuer
If there are no CA certificates issued by a CA that are part of the DOD PKI/PKE, this is a finding.

Remediation:

Obtain and install the DOD PKI CA certificate bundles by accessing the DOD PKI office website at cyber.mil/pki-pke.
Import the DOD CA certificates.

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

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

CCI-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5::SC-17 b

1.42 TCAT-AS-000710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Keystore file must be protected.

```
GROUP ID: V-222967
RULE ID: SV-222967r985893
```

Rationale:

Keystore file contains authentication information used to access application data and data resources. Access to the file must be protected.

The default location is in the .keystore file stored in the home folder of the user account used to run Tomcat, although some administrators may choose to locate the file elsewhere. The location will also be specified in the server.xml file.

Audit:

Identify the location of the .keystore file. Refer to system documentation or review the server.xml file for a specified .keystore file location.
From the Tomcat server console, run the following command to check the server.xml file:
sudo grep -i keystorefile $CATALINA_BASE/conf/server.xml
Extract the location of the file from the output.
Example:
[keystorefile=/opt/tomcat/conf/<filename.jks>]
sudo ls -la [keystorefile location]
If the file permissions are not set to 640 USER:root GROUP:tomcat, this is a finding.
If the keystore file is not stored within the tomcat folder path, i.e. [/opt/tomcat/], this is a finding.

Remediation:

Run the following commands on the Tomcat server:
sudo chmod 640 [keystorefile]
sudo chown root [keystorefile]
sudo chgrp tomcat [keystorefile]
Store the keystore file in a secured folder within the Tomcat folder path.

Additional Information:

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

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

CCI-004910 Provide protected storage for cryptographic keys with organization-defined safeguards and/or hardware protected key store.

- NIST SP 800-53 Revision 5::SC-28 (3)

1.43 TCAT-AS-000750 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Tomcat must use FIPS-validated ciphers on secured connectors.

```
GROUP ID: V-222968
RULE ID: SV-222968r961050
```

Rationale:

Connectors are how Tomcat receives requests over a network port, passes them to hosted web applications via HTTP or AJP, and then sends the results back to the requestor. Cryptographic ciphers are associated with the connector to create a secured connector. To ensure encryption strength is adequately maintained, the ciphers used must be FIPS 140-2-validated.

The FIPS-validated crypto libraries are not provided by Tomcat; they are included as part of the Java instance and the underlying Operating System. The STIG checks to ensure the FIPSMode setting is enabled for the connector and also checks the logs for FIPS errors, which indicates FIPS non-compliance at the OS or Java layers. The administrator is responsible for ensuring the OS and Java instance selected for the Tomcat installation provide and enable these FIPS modules so Tomcat can be configured to use them.

Satisfies: SRG-APP-000224-AS-000152, SRG-APP-000428-AS-000265, SRG-APP-000429-AS-000157, SRG-APP-000439-AS-000274, SRG-APP-000440-AS-000167

Audit:

From the Tomcat server console, run the following two commands to verify Tomcat server is configured to use FIPS:
sudo grep -i fipsmode $CATALINA_BASE/conf/server.xml
sudo grep -i fipsmode $CATALINA_BASE/logs/catalina.out
If server.xml does not contain FIPSMode="on", or if catalina.out contains the error "failed to set property[FIPSMODE] to [on]", this is a finding.

Remediation:

In addition to configuring Tomcat, the admin must also configure the underlying OS and Java engine to use FIPS validated encryption modules. This fix instructs how to enable FIPSMode within Tomcat, the OS and Java engine must be configured to use the FIPS validated modules according to the chosen OS and Java engine.
From the Tomcat server as a privileged user:
sudo nano $CATALINA_BASE/conf/server.xml.
In the <Listener/> element, locate the AprLifecycleListener. Either add or modify the FIPSMode setting and set it to FIPSMode="on".
EXAMPLE:
<Listener
className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on"
FIPSMode="on"
/>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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-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)

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)

1.44 TCAT-AS-000780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to JMX management interface must be restricted.

```
GROUP ID: V-222969
RULE ID: SV-222969r961095
```

Rationale:

Java Management Extensions (JMX) is used to provide programmatic access to Tomcat for management purposes. This includes monitoring and control of java applications running on Tomcat. If network access to the JMX port is not restricted, attackers can gain access to the application used to manage the system.

Audit:

Review the system security plan and network documentation. Identify the management networks that are used for system management.
From the Tomcat server as a privileged user, run the following command:
sudo grep -i jmxremote /etc/systemd/system/tomcat.service
sudo ps -ef |grep -i jmxremote
If there are no results, the JMX process is not being used, and this is not a finding.
If output includes jmxremote information, review the -Dcom.sun.management.jmxremote.host setting.
Compare the IP address associated with the JMX process with the network information in the SSP. Ensure the IP address space is dedicated for system management purposes.
If the IP address that is associated with the JMX process is not dedicated to system management usage, this is a finding.
If jmxremote is in use but the host IP address is not specified, this is a finding.

Remediation:

Make an operational determination regarding the use of JMX. If JMX management is decided upon, identify the management networks that are used for system management. Update the system security plan and network documentation with the information.
Edit the /etc/systemd/system/tomcat.service file.
Add or modify the existing CATALINA_OPTS -Dcom.sun.management.jmxremote.host setting. Set the host parameter to an IP address that is only available on a management network.
EXAMPLE:
CATALINA_OPTS='-Dcom.sun.management.jmxremote.host=192.168.0.150'
Restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl daemon-reload
Verify jmxmanagement access is restricted to the management network IP address range.

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

1.45 TCAT-AS-000790 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to Tomcat manager application must be restricted.

```
GROUP ID: V-222970
RULE ID: SV-222970r961095
```

Rationale:

The Tomcat manager application is used to manage the Tomcat server and the applications that run on Tomcat. By default, the manager application is only accessible via the localhost. Exposing the management application to any network interface that is available to non-administrative personnel leaves the Tomcat server vulnerable to attempts to access the management application. To mitigate this risk, the management application should only be run on the localhost or on network interfaces tied to a dedicated management network.

This setting is managed in the $CATALINA_BASE/conf/server.xml file.

Audit:

Review system documentation (SSP) and identify the documented management networks as well as the documented client networks. If the manager application has been deleted from the system, this is not a finding.
Run the following command as a privileged user:
sudo grep -i -A1 "RemoteAddrValve|RemoteCIDRValve" $CATALINA_BASE/webapps/manager/META-INF/context.xml
If there are no results, then no address valves exist and this is a finding.
If the Remote Address Valve settings are commented out or not configured to restrict access to localhost or the management network, this is a finding.
EXAMPLES:

- RemoteAddrValve Localhost only IPV4 and IPV6 example
  <Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="127.\d+.\d+.\d+|::1|0:0:0:0:0:0:0:1"/>
- Localhost and Management network CIDR block IPV4 and IPV6 example
  <Valve className="org.apache.catalina.valves.RemoteCIDRValve" allow="127.0.0.1, ::1",192.168.1.0/24/>

Remediation:

Update system documentation (SSP) and identify the documented management networks as well as the documented client networks.
As a privileged user, edit the $CATALINA_BASE/webapps/manager/META-INF/context.xml file.
Configure the RemoteAddrValve or RemoteCIDRValve to restrict access to the management application. This can be a restriction to the localhost or to specific management networks or hosts on the management network. Choice of address or CIDR block usage is based on operational requirements.
Order is allow from, deny from. See Tomcat Valve component documentation at the Tomcat website for specific details and additional configuration options.
Test the access restrictions once configured to assure compliance.
EXAMPLES:

- RemoteAddrValve Localhost only IPV4 and IPV6
  <Valve className="org.apache.catalina.valves.RemoteAddrValve"
  allow="127.\d+.\d+.\d+|::1|0:0:0:0:0:0:0:1"/>
- Localhost and Management network CIDR block IPV4 and IPV6
  <Valve className="org.apache.catalina.valves.RemoteCIDRValve"
  allow="127.0.0.1, ::1",192.168.1.0/24/>

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

1.45 TCAT-AS-000800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat servers must mutually authenticate proxy or load balancer connections.

```
GROUP ID: V-222971
RULE ID: SV-222971r1043178
```

Rationale:

Tomcat servers are often placed behind a proxy when exposed to both trusted and untrusted networks. This is done for security and performance reasons. Tomcat does provide an HTTP server that can be configured to make hosted applications available to clients directly. However, this HTTP server has performance limitations and is not intended to be used on an enterprise scale. Exposing this service to untrusted networks also violates the layered security model and creates elevated risk of attack. To address these issues, a proxy or load balancer can be placed in front of the Tomcat server. To ensure the proxied connection is not spoofed, SSL mutual authentication must be employed between Tomcat and the proxy.

Not all Tomcat systems will have an RMF system categorization that warrants mutual authentication protections. The site must determine if mutual authentication is warranted based on their system RMF categorization and data protection requirements. If the site determines that MA is not a requirement, they can document a risk acceptance for not mutually authenticating proxy or load balancer connections due to operational issues, or when the RMF system categorization does not warrant the added level of protection.

Audit:

Review system security plan and/or system architecture documentation and interview the system admin. Identify any proxy servers or load balancers that provide services for the Tomcat server. If there are no load balancers or proxies in use, this is not a finding. If there is a documented risk acceptance for not mutually authenticating proxy or load balancer connections due to operational issues, or RMF system categorization this is not a finding.
Using the aforementioned documentation, identify each Tomcat IP address that is served by a load balancer or proxy.
From the Tomcat server as a privileged user, review the $CATALINA_BASE/conf/server.xml file. Review each <Connector> element for the address setting and the clientAuth setting.
sudo grep -i -B1 -A5 connector $CATALINA_BASE/conf/server.xml
If a connector has a configured IP address that is proxied or load balanced and the clientAuth setting is not "true", this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
Modify each <Connector> element where the IP address is behind a proxy or load balancer.
Set clientAuth="true" then identify the applications that are associated with the connector and edit the associated web.xml files. Assure the is set to CLIENT-CERT.

Additional Information:

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

1.47 TCAT-AS-000820 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Tomcat must be configured to limit data exposure between applications.

```
GROUP ID: V-222973
RULE ID: SV-222973r1043180
```

Rationale:

If RECYCLE_FACADES is true or if a security manager is in use, a new facade object will be created for each request. This reduces the chances that a bug in an application might expose data from one request to another. This setting is configured using environment variable settings. For Linux OS flavors other than Ubuntu, use the relevant OS commands. For Ubuntu, this setting can be managed in the /etc/systemd/system/tomcat.service file via the CATALINA_OPTS variable. This setting is defined in the file and referenced during tomcat startup in order to load tomcat environment variables.

Technically, the tomcat.service referenced in the check and fix could be called a different name; but for STIG purposes and to provide a standard setting that can be referred to and obviously is used for Tomcat, tomcat.service was chosen.

Audit:

From the Tomcat server as a privileged user, run the following command:
sudo grep -i recycle_facades /etc/systemd/system/tomcat.service
If there are no results, or if the org.apache.catalina.connector. RECYCLE_FACADES is not ="true", this is a finding.

Remediation:

From the Tomcat server as a privileged user:
edit the /etc/systemd/system/tomcat.service file and either add or edit the org.apache.catalina.connector. RECYCLE_FACADES setting.
Set the org.apache.catalina.connector. RECYCLE_FACADES=true.
EXAMPLE:
Environment='CATALINA_OPTS -Dorg.apache.catalina.connector. RECYCLE_FACADES=true'
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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)

1.48 TCAT-AS-000860 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Clusters must operate on a trusted network.

```
GROUP ID: V-222974
RULE ID: SV-222974r961122
```

Rationale:

Operating a Tomcat cluster on an untrusted network creates potential for unauthorized persons to view or manipulate cluster session traffic. When operating a Tomcat cluster, care must be taken to isolate the cluster traffic from untrusted sources. Options include using a private VLAN, VPN, or IPSEC tunnel or by encrypting cluster traffic by using the EncryptInterceptor. The EncryptInterceptor adds encryption to the channel messages carrying session data between Tomcat cluster nodes.

Place the <Cluster> element inside either the <Engine> container or the <Host> container.

Placing it in the engine means supporting clustering in all virtual hosts of Tomcat and sharing the messaging component. When the user places the <Cluster> inside the <Engine> element, the cluster will append the host name of each session manager to the manager's name so that two contexts with the same name (but sitting inside two different hosts) will be distinguishable.

Audit:

Review System Security Plan (SSP) documentation determine if the Tomcat server is part of an application server cluster. Also identify Tomcat network interfaces and the proxy/load balancer that front-ends the cluster.
From the Tomcat server as a privileged user, run the following command:
sudo grep -i -A2 -B2 "Cluster" $CATALINA_BASE/conf/server.xml
If the <Cluster/> element is commented out, or there are no results returned, this requirement is NA.
If a cluster is in use, run the following command as a privileged user:
grep -i EncryptInterceptor $CATALINA_BASE/conf/server.xml file.
If the Tomcat server is clustered and the EncryptionInterceptor is not in use or if the cluster traffic is not on a private network or VLAN, this is a finding.

Remediation:

Update the System Security Plan (SSP) and document the network interface, their related IP addresses, and which interfaces transport Tomcat cluster traffic. Also document which interface is multi-cast enabled if using the McastService membership class versus Static.
To obtain the information needed for the SSP:
sudo grep -i -A3 "<Membership className" $CATALINA_BASE/conf.server.xml
Document the address="<ipAddress>" value.
Review the OS routing tables. Identify and document which interface is configured to route the Tomcat class D IP multicast traffic.
sudo netstat -r
END of Documentation instructions.
From the Tomcat server as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
sudo nano $CATALINA_BASE/conf/server.xml
Locate the <Interceptor/> element nested within the <Channel/> element.
Add the <Interceptor className="org.apache.catalina.tribes.group.interceptors.EncryptInterceptor"/> to the server.xml and save the file.
Restart the Tomcat server:
sudo systemctl restart tomcat
NOTE:
The EncryptInterceptor adds encryption to the channel messages carrying session data between nodes. This feature was added in Tomcat 9.0.13. If using the TcpFailureDetector interceptor, the EncryptInterceptor must be inserted into the interceptor chain BEFORE the TcpFailureDetector. When validating cluster members, TcpFailureDetector writes channel data directly to the other members without using the remainder of the interceptor chain, but on the receiving side, the message still goes through the chain (in reverse). Because of this asymmetry, the EncryptInterceptor must execute before the TcpFailureDetector on the sender and after it on the receiver; otherwise, message corruption will occur.

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

1.49 TCAT-AS-000920 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ErrorReportValve showServerInfo must be set to false.

```
GROUP ID: V-222975
RULE ID: SV-222975r961167
```

Rationale:

The Error Report Valve is a simple error handler for HTTP status codes that will generate and return HTML error pages. It can also be configured to return pre-defined static HTML pages for specific status codes and/or exception types. Disabling showServerInfo will only return the HTTP status code and remove all CSS from the default non-error related HTTP responses.

Audit:

As an elevated user on the Tomcat server run the following command:
sudo grep -i ErrorReportValve $CATALINA_BASE/conf/server.xml file.
If the ErrorReportValve element is not defined and showServerInfo set to "false", this is a finding.
EXAMPLE:
<Host ...>
...
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showServerInfo="false"/>
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Create or modify an ErrorReportValve <Valve> element nested beneath each <Host> element.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showServerInfo="false" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.50 TCAT-AS-000930 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Default error pages for manager application must be customized.

```
GROUP ID: V-222976
RULE ID: SV-222976r961170
```

Rationale:

Default error pages that accompany the manager application provide educational information on how to configure user accounts and groups for accessing the manager application. These error pages provide responses to 401 (Unauthorized), 403 (Forbidden), and 404 (Not Found) JSP error codes and should not exist on production systems.

Audit:

From the Tomcat server console, run the following command:
sudo cat $CATALINA_BASE/webapps/manager/WEB-INF/jsp/401.jsp
Repeat for the 402.jsp and 403.jsp files.
The default error files contain sample passwords and user accounts.
If the error files contained in this folder are not customized and sample information removed, this is a finding.

Remediation:

From the Tomcat server as a privileged user:
sudo cd $CATALINA_BASE/webapps/manager/WEB-INF/jsp/
Use a file editor like nano or vi and edit the 401, 402, and 403 jsp files. Remove account information and make the files reflect generic error information that assists users but does not provide sample data to users.
Save the file and restart Tomcat:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

1.51 TCAT-AS-000940 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ErrorReportValve showReport must be set to false.

```
GROUP ID: V-222977
RULE ID: SV-222977r961170
```

Rationale:

The Error Report Valve is a simple error handler for HTTP status codes that will generate and return HTML error pages. It can also be configured to return pre-defined static HTML pages for specific status codes and/or exception types. Disabling showReport will result in no error message or stack trace being send to the client. This setting can be tailored on a per-application basis within each application specific web.xml.

Audit:

As an elevated user on the Tomcat server run the following command:
sudo grep -i ErrorReportValve $CATALINA_BASE/conf/server.xml file.
If the ErrorReportValve element is not defined and showReport set to "false", this is a finding.
EXAMPLE:
<Host ...>
...
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showReport="false"/>
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Create or modify an ErrorReportValve <Valve> element nested beneath each <Host> element.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showReport="false" />

Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

1.52 TCAT-AS-000970 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Idle timeout for the management application must be set to 10 minutes.

```
GROUP ID: V-222979
RULE ID: SV-222979r1043182
```

Rationale:

Tomcat can set idle session timeouts on a per application basis. The management application is provided with the Tomcat installation and is used to manage the applications that are installed on the Tomcat Server. Setting the idle timeout for the management application will kill the admin user's session after 10 minutes of inactivity. This will limit the opportunity for unauthorized persons to hijack the admin session. This setting will also affect the default timeout behavior of all hosted web applications. To adjust the individual hosted application settings that are not related to management of the system, modify the individual application web.xml file if application timeout requirements differ from the STIG.

Satisfies: SRG-APP-000389, SRG-APP-000220

Audit:

If the manager application has been deleted from the system, this is not a finding.
From the Tomcat server as a privileged user, run the following commands:
sudo grep -i session-timeout $CATALINA_BASE/webapps/manager/META-INF/web.xml
sudo grep -i session-timeout
$CATALINA_BASE/conf/web.xml
If the session-timeout setting is not configured to be 10 minutes in at least one of these files, this is a finding.

Remediation:

From the Tomcat server as a privileged user:
To affect session timeout for all applications including the management application, edit the $CATALINA_BASE/conf/web.xml file.
To affect session timeout for the management application only, edit the $CATALINA_BASE/webapps/manager/META-INF/web.xml file.
Locate the session-timeout setting located within the session-config element.
Modify the session-timeout setting to be 10 minutes.
Save the file.
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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

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

1.53 TCAT-AS-001020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

LockOutRealms must be used for management of Tomcat.

```
GROUP ID: V-222980
RULE ID: SV-222980r961278
```

Rationale:

A LockOutRealm adds the ability to lock a user out after multiple failed logins. LockOutRealm is an implementation of the Tomcat Realm interface that extends the CombinedRealm to provide user lock out functionality if there are too many failed authentication attempts in a given period of time. A LockOutRealm is created by wrapping around a standard realm such as a JNDI Directory Realm which connects Tomcat to an LDAP Directory.

A Catalina container (Engine, Host, or Context) may contain no more than one Realm element (although this one Realm may itself contain multiple nested Realms). In addition, the Realm associated with an Engine or a Host is automatically inherited by lower-level containers unless the lower level container explicitly defines its own Realm. If no Realm is configured for the Engine, an instance of the Null Realm will be configured for the Engine automatically.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i LockOutRealm $CATALINA_BASE/conf/server.xml.
If there are no results or if the LockOutRealm is not used for the Tomcat management application context, this is a finding.

Remediation:

From the Tomcat server console as a privileged user edit the $CATALINA_BASE/conf/server.xml file.
sudo nano $CATALINA_BASE/conf/server.xml file
Locate or add the LockOutRealm element. Make sure the LockOutRealm element is applied to the management application at a minimum (if the management application is in use on the system). This is done by ensuring the LockOutRealm is nested under the Engine, Host or directly within the management application Context container.
EXAMPLE:

```
  <Realm className="org.apache.catalina.realm.LockOutRealm" failureCount="5"
lockOutTime="600">
```

...
</Realm>

Additional Information:

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

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

1.54 TCAT-AS-001030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

LockOutRealms failureCount attribute must be set to 5 failed logins for admin users.

```
GROUP ID: V-222981
RULE ID: SV-222981r961281
```

Rationale:

A LockOutRealm adds the ability to lock a user out after multiple failed logins. Setting the failureCount attribute to 5 will lock out a user account after 5 failed attempts.

LockOutRealm is an implementation of the Tomcat Realm interface that extends the CombinedRealm to provide user lock out functionality if there are too many failed authentication attempts in a given period of time. A LockOutRealm is created by wrapping around a standard realm such as a JNDI Directory Realm which connects Tomcat to an LDAP Directory.

A Catalina container (Engine, Host, or Context) may contain no more than one Realm element (although this one Realm may itself contain multiple nested Realms). In addition, the Realm associated with an Engine or a Host is automatically inherited by lower-level containers unless the lower level container explicitly defines its own Realm. If no Realm is configured for the Engine, an instance of the Null Realm will be configured for the Engine automatically.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i LockOutRealm $CATALINA_BASE/conf/server.xml.
If there are no results or if the LockOutRealm failureCount setting is not configured to 5, this is a finding.

Remediation:

From the Tomcat server console as a privileged user edit the $CATALINA_BASE/conf/server.xml file.
sudo nano $CATALINA_BASE/conf/server.xml file
Locate or add the LockOutRealm element. Set LockOutRealm failureCount="5"
EXAMPLE:
<Realm className="org.apache.catalina.realm.LockOutRealm" failureCount="5" lockOutTime="600">
...
</Realm>

Additional Information:

CCI-002322 Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

- NIST SP 800-53 Revision 4::AC-17 (9)
- NIST SP 800-53 Revision 5::AC-17 (9)

1.55 TCAT-AS-001040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

LockOutRealms lockOutTime attribute must be set to 600 seconds (10 minutes) for admin users.

```
GROUP ID: V-222982
RULE ID: SV-222982r961281
```

Rationale:

A LockOutRealm adds the ability to specify a lockout time that prevents further attempts after multiple failed logins. Setting the lockOutTime attribute to 600 will lock out a user account for 10 minutes. Further authentication failures during the lock out time will cause the lock out timer to reset to zero, effectively extending the lockout time. Valid authentication attempts during the lockout period will not succeed but will also not reset the lockout time.

LockOutRealm is an implementation of the Tomcat Realm interface that extends the CombinedRealm to provide user lock out functionality if there are too many failed authentication attempts in a given period of time. A LockOutRealm is created by wrapping around a standard realm such as a JNDI Directory Realm which connects Tomcat to an LDAP Directory.

A Catalina container (Engine, Host, or Context) may contain no more than one Realm element (although this one Realm may itself contain multiple nested Realms). In addition, the Realm associated with an Engine or a Host is automatically inherited by lower-level containers unless the lower level container explicitly defines its own Realm. If no Realm is configured for the Engine, an instance of the Null Realm will be configured for the Engine automatically.

Audit:

From the Tomcat server console, run the following command:
sudo grep -i LockOutRealm $CATALINA_BASE/conf/server.xml.
If there are no results or if the LockOutRealm lockOutTime setting is not configured to 600 (10 minutes), this is a finding.

Remediation:

From the Tomcat server console as a privileged user, edit the $CATALINA_BASE/conf/server.xml file.
sudo nano $CATALINA_BASE/conf/server.xml file
Locate or add the LockOutRealm element. Set lockOutTime="600"
EXAMPLE:
<Realm className="org.apache.catalina.realm.LockOutRealm" failureCount="5" lockOutTime="600">
...
</Realm>

Additional Information:

CCI-002322 Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

- NIST SP 800-53 Revision 4::AC-17 (9)
- NIST SP 800-53 Revision 5::AC-17 (9)

1.56 TCAT-AS-001050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat user account must be set to nologin.

```
GROUP ID: V-222983
RULE ID: SV-222983r961353
```

Rationale:

When installing Tomcat, a user account is created on the OS. This account is used in order for Tomcat to be able to operate on the OS but does not require the ability to actually log in to the system. Therefore when the account is created, the account must not be provided access to a login shell or other program on the system. This is done by specifying the "nologin" parameter in the command/shell field of the passwd file.

Audit:

From the command line of the Tomcat server type the following command:
sudo cat /etc/passwd|grep -i tomcat
If the command/shell field of the passwd file is not set to "/usr/sbin/nologin", this is a finding.

Remediation:

From the Tomcat command line type the following command:
sudo usermod -s /usr/sbin/nologin tomcat

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)

1.57 TCAT-AS-001060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat user account must be a non-privileged user.

```
GROUP ID: V-222984
RULE ID: SV-222984r961353
```

Rationale:

Use a distinct non-privileged user account for running Tomcat. If Tomcat processes are compromised and a privileged user account is used to operate the Tomcat server processes, the entire system becomes compromised.

Sample passwd file: tomcat:x:1001:1001::/opt/tomcat/usr/sbin/nologin

The user ID is stored in field 3 of the passwd file.

Audit:

Run the following command to identify the Tomcat process UID:
ps -ef | { head -1; grep catalina; } | cut -f1 -d" "
Run the following command to obtain the OS user ID tied to the Tomcat process:
cat /etc/passwd|grep -i <UID>|cut -f3 -d:
Unless operationally necessary, the Tomcat process should not be tied to a privileged OS user ID. Depending on the operating system, privileged OS user IDs will typically be assigned user ID values <500 or <1000.
If the Tomcat process is running as a privileged user and is not documented and approved, this is a finding.
If the user ID field of the passwd file is set to 0, this is a finding.

Remediation:

From the Tomcat server, create a tomcat user by adding a new non-privileged user OS account with the following command:
sudo useradd tomcat
Edit the systemd tomcat.service file or create one if it does not exist. Use the new "tomcat" user account by setting; USER=tomcat
Location of the file should be /etc/systemd/system/tomcat.service.
Enable the Tomcat service:
sudo restorecon /etc/systemd/system/tomcat.service
sudo chmod 644 /etc/systemd/system/tomcat.service
sudo systemctl enable tomcat.service
Start Tomcat:
sudo systemctl start tomcat

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)

1.58 TCAT-AS-001080 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Application user name must be logged.

```
GROUP ID: V-222985
RULE ID: SV-222985r961362
```

Rationale:

The access logfile format is defined within a Valve that implements the org.apache.catalina.valves.AccessLogValve interface within the /opt/tomcat/server.xml configuration file: The %u pattern code is included in the pattern element and logs the username used to authenticate to an application. Including the username pattern in the log configuration provides useful information about the application user who is logging in, which is critical for troubleshooting and forensic investigations.

Audit:

As an elevated user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Review all "Valve" elements.
If the pattern= statement does not include %u, this is a finding.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>

Remediation:

As a privileged user on the Tomcat server:
Edit the $CATALINA_BASE/conf/server.xml file.
Modify the <Valve> element that is nested beneath the <Host> element. Change the AccessLogValve setting to include %u in the pattern= statement.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

Additional Information:

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)

1.59 TCAT-AS-001200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_HOME folder must be owned by the root user, group tomcat.

```
GROUP ID: V-222986
RULE ID: SV-222986r961461
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have the folder where Tomcat is installed owned by the root user with the group set to tomcat. The $CATALINA_HOME environment variable should be set to the location of the root directory of the "binary" distribution of Tomcat.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_HOME -follow -maxdepth 0 (! -user root -o ! -group tomcat) -ls
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_HOME folder ownership and group membership is not set to root:tomcat, this is a finding.

Remediation:

Run the following commands on the Tomcat server:
sudo find $CATALINA_HOME -maxdepth 0 (! -user root) | sudo xargs chown root
sudo find $CATALINA_HOME -maxdepth 0 (! -group tomcat) | sudo xargs chgrp tomcat

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)

1.60 TCAT-AS-001220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_BASE/conf/ folder must be owned by root, group tomcat.

```
GROUP ID: V-222987
RULE ID: SV-222987r961461
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have Tomcat files contained in the conf/ folder as members of the "tomcat" group. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions. Note that running Tomcat in a Docker environment can impact how file permissions and user ownership settings are applied. Due to associated Docker configuration complexities, the STIG is scoped for standalone rather than virtual Docker deployments.

If the ISSM determines the operational need to allow application admins access to change the Tomcat configuration outweighs the risk of limiting that access, then they can change the group membership to accommodate. Ownership must not be changed. The ISSM should take the exposure of the system to high risk networks into account.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/conf -follow -maxdepth 0 (! -user root -o ! -group tomcat) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the group permissions are set in accordance with the risk acceptance. Ownership must not be changed.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/conf folder ownership and group membership is not set to root:tomcat, this is a finding.

Remediation:

If operational/application requirements specify different group file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance. Ownership must not be changed.
Run the following commands on the Tomcat server:
sudo find $CATALINA_BASE/conf -maxdepth 0 (! -user root) | sudo xargs chown root
sudo find $CATALINA_BASE/conf -maxdepth 0 (! -group tomcat) | sudo xargs chgrp tomcat

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)

1.61 TCAT-AS-001260 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

$CATALINA_BASE/temp/ folder must be owned by tomcat user, group tomcat.

```
GROUP ID: V-222989
RULE ID: SV-222989r961461
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

If operational needs require application administrators to be able to change application configurations, the group permissions can be modified to allow specific application admins the access they require with an ISSM risk acceptance. Ownership may not change. The exposure of the system to high risk networks should always be taken into account.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/temp -follow -maxdepth 0 (! -user tomcat -o ! -group tomcat) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/temp folder ownership and group membership is not set to tomcat:tomcat, this is a finding.

Remediation:

If operational/application requirements specify different file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following commands on the Tomcat server:
sudo find $CATALINA_BASE/temp -maxdepth 0 (! -user tomcat) | sudo xargs chown tomcat
sudo find $CATALINA_BASE/temp -maxdepth 0 (! -group tomcat) | sudo xargs chgrp tomcat

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)

1.61 TCAT-AS-001250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_BASE/logs/ folder must be owned by tomcat user, group tomcat.

```
GROUP ID: V-222988
RULE ID: SV-222988r961461
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/logs -follow -maxdepth 0 (! -user tomcat -o ! -group tomcat) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/logs folder ownership and group membership is not set to tomcat:tomcat, this is a finding.

Remediation:

If operational/application requirements specify different group file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following commands on the Tomcat server:
sudo find $CATALINA_BASE/logs -maxdepth 0 (! -user tomcat) | sudo xargs chown tomcat
sudo find $CATALINA_BASE/logs -maxdepth 0 (! -group tomcat) | sudo xargs chgrp tomcat

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)

1.63 TCAT-AS-001270 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

$CATALINA_BASE/temp folder permissions must be set to 750.

```
GROUP ID: V-222990
RULE ID: SV-222990r961461
```

Rationale:

Tomcat's file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with the group Tomcat. While root has read/write privileges, tomcat group only has read and world has no permissions. The exceptions are the logs, temp and work directory that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

If operational needs require application administrators to be able to change application configurations, the group permissions can be modified to allow specific application admins the access they require with an ISSM risk acceptance. Ownership may not change.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/temp -follow -maxdepth 0 -type d (! -perm 750) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/temp folder permissions are not set to 750, this is a finding.

Remediation:

If operational/application requirements specify different file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following commands on the Tomcat server:
sudo find $CATALINA_BASE/temp -follow -maxdepth 0 -type d -print0 | sudo xargs chmod 750 $CATALINA_BASE/temp

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)

1.64 TCAT-AS-001280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

$CATALINA_BASE/work/ folder must be owned by tomcat user, group tomcat.

```
GROUP ID: V-222991
RULE ID: SV-222991r961461
```

Rationale:

Tomcat file permissions must be restricted. The standard configuration is to have all Tomcat files owned by root with group Tomcat. While root has read/write privileges, group only has read permissions, and world has no permissions. The exceptions are the logs, temp, and work directories that are owned by the Tomcat user rather than root. This means that even if an attacker compromises the Tomcat process, they cannot change the Tomcat configuration, deploy new web applications, or modify existing web applications. The Tomcat process runs with a umask of 0027 to maintain these permissions.

If operational needs require application administrators to be able to change application configurations, the group permissions can be modified to allow specific application admins the access they require with an ISSM risk acceptance. Ownership may not change.

Audit:

Access the Tomcat server from the command line and execute the following OS command:
sudo find $CATALINA_BASE/work -follow -maxdepth 0 (! -user tomcat -o ! -group tomcat) -ls
If ISSM risk acceptance specifies deviation from requirement based on operational/application needs, this is not a finding if the permissions are set in accordance with the risk acceptance.
If no folders are displayed, this is not a finding.
If results indicate the $CATALINA_BASE/work folder ownership and group membership is not set to tomcat:tomcat, this is a finding.

Remediation:

If operational/application requirements specify different group file permissions, obtain ISSM risk acceptance and set permissions according to risk acceptance.
Run the following commands on the Tomcat server:
sudo find $CATALINA_BASE/work -maxdepth 0 (! -user tomcat) | sudo xargs chown tomcat
sudo find $CATALINA_BASE/work -maxdepth 0 (! -group tomcat) | sudo xargs chgrp tomcat

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)

1.65 TCAT-AS-001320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Multifactor certificate-based tokens (CAC) must be used when accessing the management interface.

```
GROUP ID: V-222993
RULE ID: SV-222993r985888
```

Rationale:

Password authentication does not provide sufficient security control when accessing a management interface. DOD has specified that a CAC will be used when authenticating and passwords will only be used when CAC authentication is not a plausible solution. Tomcat provides the ability to do certificate based authentication and client authentication; therefore, the Tomcat server must be configured to use CAC.

Satisfies: SRG-APP-000391-AS-000239, SRG-APP-000392-AS-000240, SRG-APP-000402-AS-000247, SRG-APP-000403-AS-000248

Audit:

If the manager application has been deleted from the Tomcat server, this is not a finding. From the Tomcat server as a privileged user, issue the following command:
sudo grep -i auth-method $CATALINA_BASE/webapps/manager/WEB-INF/web.xml
If the <Auth-Method> for the web manager application is not set to CLIENT-CERT, this is a finding.

Remediation:

From the Tomcat server as a privileged user, edit the $CATALINA_BASE/webapps/manager/WEB-INF/web.xml file and modify the auth-method for the manager application security constraint.
sudo nano $CATALINA_BASE/webapps/manager/WEB-INF/web.xml
Locate contained within the section, modify to specify CLIENT-CERT.
EXAMPLE:
CLIENT-CERT
In addition, the connector used for accessing the manager application must be configured to require client authentication by setting clientAuth="true" and the manager application roles must be configured in the LDAP server.
Restart the Tomcat server:
sudo systemctl restart tomcat

Additional Information:

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

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)

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

1.66 TCAT-AS-001430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Certificates in the trust store must be issued/signed by an approved CA.

```
GROUP ID: V-222994
RULE ID: SV-222994r961596
```

Rationale:

Use of self-signed certificates creates a lack of integrity and invalidates the certificate based authentication trust model. Certificates used by production systems must be issued/signed by a trusted Root CA and cannot be self-signed. For systems that communicate with industry partners, the DoD ECA program supports the issuance of DoD-approved certificates to industry partners. For information on the DoD ECA program, refer to the DoD PKI office. Links to their site are available on https://public.cyber.mil.

Audit:

For the systemd Ubuntu OS, check the tomcat.service file to read the content of the JAVA_OPTS environment variable setting.
sudo cat /etc/systemd/system/tomcat.service |grep -i truststore
EXAMPLE output:
set JAVA_OPTS="-Djavax.net.ssl.trustStore=/path/to/truststore" "-Djavax.net.ssl.trustStorePassword=**********"
If the variable is not set, use the default location command below. If the variable is set, use the alternate location command below and include the path and truststore file.
-Default location:
keytool -list -cacerts -v | grep -i issuer
-Alternate location:
keytool -list -keystore -v |grep -i issuer
If there are no CA certificates issued by a Certificate Authority (CA) that is part of the DoD PKI/PKE, this is a finding.

Remediation:

Obtain and install the DoD PKI CA certificate bundles by accessing the DoD PKI office website at https://cyber.mil/pki-pke.
Download the certificate bundles and then use certificate management utilities such as keytool or openssl to import the DoD CA certificates into the trust store.

Additional Information:

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)

1.67 TCAT-AS-001460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application server, when categorized as a high availability system within RMF, must be in a high-availability (HA) cluster.

```
GROUP ID: V-222995
RULE ID: SV-222995r961620
```

Rationale:

A MAC I system is a system that handles data vital to the organization's operational readiness or effectiveness of deployed or contingency forces. A MAC I system must maintain the highest level of integrity and availability. By HA clustering the application server, the hosted application and data are given a platform that is load-balanced and provided high-availability.

Audit:

This requirement only applies to a system that is categorized as high within the Risk Management Framework (RMF).
Review the System Security Plan (SSP) or other system documentation that specifies the operational uptime requirements and RMF system categorization.
If the system is categorized as high, from the Tomcat server as a privileged user, run the following command:
sudo grep -i -A10 -B2 "Cluster" $CATALINA_BASE/conf/server.xml
If the <Cluster/> element is commented out, or no results returned, then the system is not clustered and this is a finding.

Remediation:

From the Tomcat server as a privileged user, modify the $CATALINA_BASE/conf/server.xml file.
Uncomment the "<Cluster/> object and configure the system into a cluster as per the Tomcat clustering documentation provided at the Tomcat website.
https://tomcat.apache.org/tomcat-9.0-doc/config/cluster.html

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

1.68 TCAT-AS-001470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat server must be patched for security vulnerabilities.

```
GROUP ID: V-222996
RULE ID: SV-222996r1067548
```

Rationale:

Tomcat is constantly being updated to address newly discovered vulnerabilities, some of which include denial-of-service attacks. To address this risk, the Tomcat administrator must ensure the system remains up to date on patches.

Satisfies: SRG-APP-000435-AS-000163, SRG-APP-000456-AS-000266

Audit:

Refer to https://tomcat.apache.org/security-9.html and identify the latest secure version of Tomcat with no known vulnerabilities.
As a privileged user from the Tomcat server, run the following command:
sudo $CATALINA_HOME/bin/version.sh |grep -i server
Compare the version running on the system to the latest secure version of Tomcat.
Note: If TCAT-AS-000950 is compliant, users may need to leverage a different management interface. There is commonly a version.bat script in CATALINA_HOME/bin that will also output the current version of Tomcat.
If the version is more than one version behind the most recent patch level, this is a finding.

Remediation:

Follow operational procedures for upgrading Tomcat. Download latest version of Tomcat and install in a test environment. Test applications that are running in production and follow all operations best practices when upgrading the production Tomcat application servers.
Update the Tomcat production instance accordingly and ensure corrected builds are installed once tested and verified.

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

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

1.69 TCAT-AS-001560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

AccessLogValve must be configured for Catalina engine.

```
GROUP ID: V-222997
RULE ID: SV-222997r1016518
```

Rationale:

The <Engine> container represents the entire request processing machinery associated with a particular Catalina Service. It receives and processes all requests from one or more connectors, and returns the completed response to the connector for transmission back to the client. The AccessLogValve will log activity for the Catalina service.

Exactly one engine element MUST be nested inside a service element, following all of the corresponding connector elements associated with the service.

Satisfies: SRG-APP-000495-AS-000220, SRG-APP-000381-AS-000089, SRG-APP-000499-AS-000224, SRG-APP-000504-AS-000229

Audit:

As an elevated user on the Tomcat server, edit the $CATALINA_BASE/conf/server.xml file.
Review the <Engine> element. Ensure one AccessLog <Valve> element is nested within the engine element.
If a <Valve className="org.apache.catalina.valves.AccessLogValve" .../> element is not defined, this is a finding.
EXAMPLE:
<Engine name="Standalone" ...>
...
<Valve className="org.apache.catalina.valves.AccessLogValve"
prefix="catalina_access_log" suffix=".txt"
pattern="common"/>
...
</Engine>

Remediation:

As a privileged user on the Tomcat server, edit the $CATALINA_BASE/conf/server.xml file.
Create a <Valve> element that is nested beneath the <Host> element containing an AccessLogValve.
EXAMPLE:
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="false">
...
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %t %u "%r" %s %b" />
...
</Host>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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-003938 Automatically generate audit records of the enforcement actions.

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

CCI-001814 The Information system supports auditing of the enforcement actions.

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

1.70 TCAT-AS-001590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Changes to $CATALINA_HOME/bin/ folder must be logged.

```
GROUP ID: V-222998
RULE ID: SV-222998r961827
```

Rationale:

The $CATALINA_HOME/bin folder contains startup and control scripts for the Tomcat Catalina server. To provide forensic evidence in the event of file tampering, changes to content in this folder must be logged. For Linux OS flavors other than Ubuntu, use the relevant OS commands. This can be done on the Ubuntu OS via the auditctl command. Using the -p wa flag set the permissions flag for a file system watch and logs file attribute and content change events into syslog.

Audit:

Run the following commands From the Tomcat server as a privileged user:
Identify the home folder for the Tomcat server.
sudo grep -i -- 'catalina_home|catalina_base' /etc/systemd/system/tomcat.service
Check the audit rules for the Tomcat folders.
sudo auditctl -l $CATALINA_HOME/bin |grep -i bin
If the results do not include -w $CATALINA_HOME/bin -p wa -k tomcat, or if there are no results, this is a finding.

Remediation:

From the Tomcat server as a privileged user, use the auditctl command.
sudo auditctl -w $CATALINA_HOME/bin -p wa -k tomcat
Validate the audit watch was created.
sudo auditctl -l
The user should see:
-w $CATALINA_HOME/ -p wa -k tomcat

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

1.71 TCAT-AS-001591 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Changes to $CATALINA_BASE/conf/ folder must be logged.

```
GROUP ID: V-222999
RULE ID: SV-222999r961827
```

Rationale:

The $CATALINA_BASE/conf folder contains configuration files for the Tomcat Catalina server. To provide forensic evidence in the event of file tampering, changes to contents in this folder must be logged. For Linux OS flavors other than Ubuntu, use the relevant OS commands. This can be done on the Ubuntu OS via the auditctl command. Using the -p wa flag set the permissions flag for a file system watch and logs file attribute and content change events into syslog.

Audit:

Run the following commands From the Tomcat server as a privileged user:
Identify the home folder for the Tomcat server.
sudo grep -i -- 'catalina_home|catalina_base' /etc/systemd/system/tomcat.service
Check the audit rules for the Tomcat folders.
sudo auditctl -l $CATALINA_HOME/bin |grep -i conf
If the results do not include -w $CATALINA_BASE/conf -p wa -k tomcat, or if there are no results, this is a finding.

Remediation:

From the Tomcat server as a privileged user, use the auditctl command.
sudo auditctl -w $CATALINA_BASE/conf -p wa -k tomcat
Validate the audit watch was created.
sudo auditctl -l
The user should see:
-w $CATALINA_HOME/ -p wa -k tomcat

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

1.72 TCAT-AS-001592 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Changes to $CATALINA_HOME/lib/ folder must be logged.

```
GROUP ID: V-223000
RULE ID: SV-223000r961827
```

Rationale:

The $CATALINA_HOME/lib folder contains library files for the Tomcat Catalina server. These are in the form of java archive (jar) files. To provide forensic evidence in the event of file tampering, changes to contents in this folder must be logged. For Linux OS flavors other than Ubuntu, use the relevant OS commands. This can be done on the Ubuntu OS via the auditctl command. Using the -p wa flag set the permissions flag for a file system watch and logs file attribute and content change events into syslog.

Audit:

Run the following commands From the Tomcat server as a privileged user:
Identify the home folder for the Tomcat server.
sudo grep -i -- 'catalina_home|catalina_base' /etc/systemd/system/tomcat.service
Check the audit rules for the Tomcat folders
sudo auditctl -l $CATALINA_HOME/bin |grep -i lib
If the results do not include -w $CATALINA_HOME/lib -p wa -k tomcat, or if there are no results, this is a finding.

Remediation:

From the Tomcat server as a privileged user, use the auditctl command.
sudo auditctl -w $CATALINA_HOME/lib -p wa -k tomcat
Validate the audit watch was created.
sudo auditctl -l
The user should see:
-w $CATALINA_HOME/ -p wa -k tomcat

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

1.73 TCAT-AS-001640 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Application servers must use NIST-approved or NSA-approved key management technology and processes.

```
GROUP ID: V-223001
RULE ID: SV-223001r961857
```

Rationale:

Class 3 PKI certificates are used for servers and software signing rather than for identifying individuals. Class 4 certificates are used for business-to-business transactions. Utilizing unapproved certificates not issued or approved by DoD or CNS creates an integrity risk. The application server must utilize approved DoD or CNS Class 3 or Class 4 certificates for software signing and business-to-business transactions.

Audit:

For the systemd Ubuntu OS, check the tomcat.service file to read the content of the JAVA_OPTS environment variable setting.
sudo cat /etc/systemd/system/tomcat.service |grep -i truststore
EXAMPLE output:
set JAVA_OPTS="-Djavax.net.ssl.trustStore=/path/to/truststore" "-Djavax.net.ssl.trustStorePassword=**********"
If the variable is not set, use the default location command below. If the variable is set, use the alternate location command below and include the path and truststore file.
-Default location:
keytool -list -cacerts -v | grep -i issuer
-Alternate location:
keytool -list -keystore -v |grep -i issuer
If there are no CA certificates issued by a Certificate Authority (CA) that is part of the DoD PKI/PKE, this is a finding.

Remediation:

Obtain and install the DoD PKI CA certificate bundles by accessing the DoD PKI office website at cyber.mil/pki-pke.
Import the DoD CA certificates.

Additional Information:

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

1.74 TCAT-AS-001660 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

STRICT_SERVLET_COMPLIANCE must be set to true.

```
GROUP ID: V-223002
RULE ID: SV-223002r961863
```

Rationale:

Strict Servlet Compliance forces Tomcat to adhere to standards specifications including but not limited to RFC2109. RFC2109 sets the standard for HTTP session management. This setting affects several settings which primarily pertain to cookie headers, cookie values, and sessions. Cookies will be parsed for strict adherence to specifications.

Note that changing a number of these default settings may break some systems, as some browsers are unable to correctly handle the cookie headers that result from a strict adherence to the specifications.

This one setting changes the default values for the following settings:

org.apache.catalina.core. ApplicationContext.GET_RESOURCE_REQUIRE_SLASH
org.apache.catalina.core. ApplicationDispatcher.WRAP_SAME_OBJECT
org.apache.catalina.core. StandardHostValve.ACCESS_SESSION
org.apache.catalina.session. StandardSession.ACTIVITY_CHECK
org.apache.catalina.session. StandardSession.LAST_ACCESS_AT_START
org.apache.tomcat.util.http. ServerCookie.ALWAYS_ADD_EXPIRES
org.apache.tomcat.util.http. ServerCookie.FWD_SLASH_IS_SEPARATOR
org.apache.tomcat.util.http. ServerCookie.PRESERVE_COOKIE_HEADER
org.apache.tomcat.util.http. ServerCookie.STRICT_NAMING The resourceOnlyServlets attribute of any Context element. The tldValidation attribute of any Context element. The useRelativeRedirects attribute of any Context element. The xmlNamespaceAware attribute of any Context element. The xmlValidation attribute of any Context element.

Audit:

If the system has an ISSM risk acceptance for operational issues that arise due to this setting, this is not a finding.
From the Tomcat server as a privileged user, run the following command:
sudo grep -i strict_servlet /etc/systemd/system/tomcat.service
If there are no results, or if the
-Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE is not set to true, this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Edit the /etc/systemd/system/tomcat.service file and either add or edit the org.apache.catalina.STRICT_SERVLET_COMPLIANCE setting.
Set the org.apache.catalina.STRICT_SERVLET_COMPLIANCE=true
EXAMPLE:
CATALINA_OPTS='-Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true'
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.75 TCAT-AS-001670 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

RECYCLE_FACADES must be set to true.

```
GROUP ID: V-223003
RULE ID: SV-223003r961863
```

Rationale:

If RECYCLE_FACADES is true or if a security manager is in use, a new facade object will be created for each request. This reduces the chances that a bug in an application might expose data from one request to another. This setting is configured using environment variable settings. For Linux OS flavors other than Ubuntu, use the relevant OS commands. For Ubuntu, this setting can be managed in the /etc/systemd/system/tomcat.service file via the CATALINA_OPTS variable. This setting is defined in the file and referenced during Tomcat startup in order to load Tomcat environment variables.

Technically, the tomcat.service referenced in the check and fix could be called a different name, for STIG purposes and to provide a standard setting that can be referred to and obviously is used for Tomcat, tomcat.service was chosen.

Audit:

From the Tomcat server as a privileged user, run the following command:
sudo grep -i recycle_facades /etc/systemd/system/tomcat.service
If there are no results, or if the org.apache.catalina.connector. RECYCLE_FACADES is not ="true", this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Edit the /etc/systemd/system/tomcat.service file and either add or edit the org.apache.catalina.connector. RECYCLE_FACADES setting.
Set the org.apache.catalina.connector. RECYCLE_FACADES=true
EXAMPLE:
Environment='CATALINA_OPTS -Dorg.apache.catalina.connector. RECYCLE_FACADES=true'
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.76 TCAT-AS-001680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ALLOW_BACKSLASH must be set to false.

```
GROUP ID: V-223004
RULE ID: SV-223004r961863
```

Rationale:

When Tomcat is installed behind a proxy configured to only allow access to certain Tomcat contexts (web applications), an HTTP request containing "/../" may allow attackers to work around the proxy restrictions using directory traversal attack methods. If allow_backslash is true the '' character will be permitted as a path delimiter. The default value for the setting is false but Tomcat should always be configured as if no proxy restricting context access was used and allow_backslash should be set to false to prevent directory traversal style attacks. This setting can create operability issues with non-compliant clients. In order to accommodate a non-compliant client, any deviation from the STIG setting must be approved by the ISSO.

Audit:

If the ISSO has accepted the risk for enabling the ALLOW_BACKSLASH setting, this requirement is NA.
From the Tomcat server as an elevated user, run the following command:
sudo grep -i ALLOW_BACKSLASH $CATALINA_BASE/conf/catalina.properties
sudo grep -i catalina_opts /etc/systemd/system/tomcat.service
If org.apache.catalina.connector. ALLOW_BACKSLASH=true, this is a finding.

Remediation:

As a privileged user on the Tomcat server:
If the finding is in the catalina.properties file, edit the $CATALINA_BASE/conf/catalina.properties file.
sudo nano $CATALINA_BASE/conf/catalina.properties
Change the org.apache.catalina.connector.ALLOW_BACKSLASH=true setting to =false.
If the finding is in the /etc/systemd/services/tomcat/service file, edit the file using a text editor.
sudo nano /etc/systemd/services/tomcat.service
Locate the "Environment='CATALINA_OPTS=' line and change the -D.org.apache.catalina.connectorALLOW_BACKSLASH=true setting to =false.
Restart Tomcat by running the following commands:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.77 TCAT-AS-001690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ENFORCE_ENCODING_IN_GET_WRITER must be set to true.

```
GROUP ID: V-223005
RULE ID: SV-223005r961863
```

Rationale:

Some clients try to guess the character encoding of text media when the mandated default of ISO-8859-1 should be used. Some browsers will interpret as UTF-7 when the characters are safe for ISO-8859-1. This can create the potential for a XSS attack. To defend against this, enforce_encoding_in_get_writer must be set to true.

Audit:

From the Tomcat server as a privileged user, run the following command:
sudo grep -i enforce_encoding /etc/systemd/system/tomcat.service
If there are no results, or if the org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER is not ="true", this is a finding.

Remediation:

From the Tomcat server as a privileged user:
Edit the /etc/systemd/system/tomcat.service file, and either add or edit the org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER setting.
Set the org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER=true
EXAMPLE:
Environment='CATALINA_OPTS -Dorg.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER=true'
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.78 TCAT-AS-001700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tomcat users in a management role must be approved by the ISSO.

```
GROUP ID: V-223006
RULE ID: SV-223006r961863
```

Rationale:

Deploying applications to Tomcat requires a Tomcat user account that is in the "manager-script" role. Any user accounts in a Tomcat management role must be approved by the ISSO.

Audit:

Review the Tomcat servers System Security Plan/server documentation.
Ensure that user accounts and roles with access to Tomcat management features such as the "manager-script" role are documented and approved by the ISSO.
If the ISSO has not approved of documented roles and users who have management rights to the Tomcat server, this is a finding.

Remediation:

Document the users and the roles that have been defined for use with the Tomcat server.
Ensure that all users and roles with access to Tomcat management features and capabilities are approved by the ISSO.

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

1.79 TCAT-AS-001710 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Hosted applications must be documented in the system security plan.

```
GROUP ID: V-223007
RULE ID: SV-223007r961863
```

Rationale:

The ISSM/ISSO must be cognizant of all applications operating on the Tomcat server, and must address any security implications associated with the operation of the applications.

If unknown/undocumented applications are operating on the Tomcat server, these applications increase risk for the system due to not being managed, patched or monitored for unapproved activity on the system.

Audit:

Review the Tomcat servers System Security Plan/server documentation.
Access the Tomcat server and review the $CATALINA_BASE/webapps folder.
Ensure that all webapps are documented in the SSP.
If the applications that are hosted on the Tomcat server are not documented in the SSP, this is a finding.

Remediation:

Document the applications that have an ATO on the Tomcat server.
Retain the information in the SSP and present to the auditor in the event of a CCRI.

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

1.80 TCAT-AS-001720 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Connectors must be approved by the ISSO.

```
GROUP ID: V-223008
RULE ID: SV-223008r961863
```

Rationale:

Connectors are how Tomcat receives requests over a network port, passes them to hosted web applications via HTTP or AJP and then sends back the results to the requestor. A port and a protocol are tied to each connector. Only connectors approved by the ISSO must be installed. ISSO review will consist of validating connector protocol as being secure and required in order for the hosted application to operate. The ISSO will ensure that unnecessary or insecure connector protocols are not enabled. The ISSO will provide documented approval for each connector that will be maintained in the System Security Plan (SSP).

Audit:

Review the Tomcat servers System Security Plan/server documentation.
Access the Tomcat server and review the server.xml file.
grep -i "connector port" $CATALINA_BASE/conf/server.xml
Compare the active Connectors and their associated IP ports with the Connectors documented and approved in the SSP.
If the Connectors that are configured on the Tomcat server are not approved by the ISSO and documented in the SSP, this is a finding.

Remediation:

Document and obtain ISSO approval for the Connectors that are configured on the Tomcat server.
Retain the information in the SSP and present to the auditor in the event of a CCRI.

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

1.81 TCAT-AS-001730 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Connector address attribute must be set.

```
GROUP ID: V-223009
RULE ID: SV-223009r961863
```

Rationale:

Connectors are how Tomcat receives requests over a network port, passes them to hosted web applications via HTTP or AJP, and then sends back the results to the requestor. The "address" attribute specifies which network interface the connector listens on. If no IP address is specified, the connector will listen on all configured interfaces. Access to the connector must be restricted to only the network interface(s) specified in the System Security Plan (SSP).

Audit:

Review SSP documentation for list of approved connectors and associated TCP/IP ports and interfaces.
Verify the address attribute is specified for each connector and is set to the network interface specified in the SSP.
Execute the following command to find configured Connectors:
sudo grep -i -B1 -A5 connector $CATALINA_BASE/conf/server.xml
Review results and examine the "address=" field for each connector.
If the connector address attribute is not specified as per the SSP, this is a finding.

Remediation:

Ensure the address attribute for each connector and the network interfaces are specified in the SSP.
Edit the following file From the Tomcat server as a privileged user:
$CATALINA_BASE/conf/server.xml
Locate each Connector element then edit or add the "address=" field for each connector and specify the appropriate network IP address. The following is an example using a random IP address:
EXAMPLE:
<Connector
port="8443"
address="192.168.0.145"
...
/>
Restart the Tomcat server:
sudo systemctl restart tomcat
sudo systemctl daemon-reload

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

1.82 TCAT-AS-001731 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application server must alert the system administrator (SA) and information system security offer (ISSO), at a minimum, in the event of a log processing failure.

```
GROUP ID: V-223010
RULE ID: SV-223010r985887
```

Rationale:

Logs are essential to monitor the health of the system, investigate changes that occurred to the system, or investigate a security incident. When log processing fails, the events during the failure can be lost. To minimize the timeframe of the log failure, an alert needs to be sent to the SA and ISSO at a minimum.

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.

Audit:

This requirement cannot be met by the Tomcat server natively and must be done at the OS. Review the operating system. Ensure the OS is configured to alert the ISSO and SA in the event of an audit processing failure.
The alert notification method itself can be accomplished in a variety of ways and is not restricted to email alone. The intention is to send an alert; the method used to send the alert is not a factor of the requirement. The fix uses email but other alert methods are acceptable.
If the OS is not configured to alert the ISSO and SA in the event of an audit processing failure, this is a finding.

Remediation:

Procedures for meeting this requirement will vary according to the OS. For Ubuntu Linux systems, instructions for notifying via email are provided. Other alert methods are also acceptable but are not provided here.
Configure "auditd" service to notify the SA and ISSO in the event of an audit processing failure.
Edit the following line in "/etc/audit/auditd.conf" to ensure that administrators are notified via email for those situations:
action_mail_acct = root
Restart the auditd service so the changes take effect:

sudo systemctl restart auditd.service

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

CCI-003831 Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

- NIST SP 800-53 Revision 5::AU-9 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	TCAT-AS-000020 (Manual)	☐	☐
1.2	TCAT-AS-000010 (Manual)	☐	☐
1.3	TCAT-AS-000030 (Manual)	☐	☐
1.4	TCAT-AS-000040 (Manual)	☐	☐
1.5	TCAT-AS-000050 (Manual)	☐	☐
1.6	TCAT-AS-000060 (Manual)	☐	☐
1.7	TCAT-AS-000080 (Manual)	☐	☐
1.8	TCAT-AS-000070 (Manual)	☐	☐
1.9	TCAT-AS-000090 (Manual)	☐	☐
1.10	TCAT-AS-000100 (Manual)	☐	☐
1.11	TCAT-AS-000110 (Manual)	☐	☐
1.12	TCAT-AS-000170 (Manual)	☐	☐
1.13	TCAT-AS-000180 (Manual)	☐	☐
1.14	TCAT-AS-000240 (Manual)	☐	☐
1.15	TCAT-AS-000250 (Manual)	☐	☐
1.16	TCAT-AS-000260 (Manual)	☐	☐
1.17	TCAT-AS-000270 (Manual)	☐	☐
1.18	TCAT-AS-000360 (Manual)	☐	☐
1.19	TCAT-AS-000361 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	TCAT-AS-000370 (Manual)	☐	☐
1.21	TCAT-AS-000371 (Manual)	☐	☐
1.22	TCAT-AS-000380 (Manual)	☐	☐
1.23	TCAT-AS-000390 (Manual)	☐	☐
1.24	TCAT-AS-000450 (Manual)	☐	☐
1.25	TCAT-AS-000470 (Manual)	☐	☐
1.26	TCAT-AS-000490 (Manual)	☐	☐
1.27	TCAT-AS-000500 (Manual)	☐	☐
1.28	TCAT-AS-000510 (Manual)	☐	☐
1.29	TCAT-AS-000520 (Manual)	☐	☐
1.30	TCAT-AS-000530 (Manual)	☐	☐
1.31	TCAT-AS-000540 (Manual)	☐	☐
1.32	TCAT-AS-000550 (Manual)	☐	☐
1.33	TCAT-AS-000560 (Manual)	☐	☐
1.34	TCAT-AS-000570 (Manual)	☐	☐
1.35	TCAT-AS-000580 (Manual)	☐	☐
1.36	TCAT-AS-000590 (Manual)	☐	☐
1.37	TCAT-AS-000600 (Manual)	☐	☐
1.38	TCAT-AS-000610 (Manual)	☐	☐
1.39	TCAT-AS-000630 (Manual)	☐	☐
1.40	TCAT-AS-000690 (Manual)	☐	☐
1.41	TCAT-AS-000700 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	TCAT-AS-000710 (Manual)	☐	☐
1.43	TCAT-AS-000750 (Manual)	☐	☐
1.44	TCAT-AS-000780 (Manual)	☐	☐
1.45	TCAT-AS-000790 (Manual)	☐	☐
1.45	TCAT-AS-000800 (Manual)	☐	☐
1.47	TCAT-AS-000820 (Manual)	☐	☐
1.48	TCAT-AS-000860 (Manual)	☐	☐
1.49	TCAT-AS-000920 (Manual)	☐	☐
1.50	TCAT-AS-000930 (Manual)	☐	☐
1.51	TCAT-AS-000940 (Manual)	☐	☐
1.52	TCAT-AS-000970 (Manual)	☐	☐
1.53	TCAT-AS-001020 (Manual)	☐	☐
1.54	TCAT-AS-001030 (Manual)	☐	☐
1.55	TCAT-AS-001040 (Manual)	☐	☐
1.56	TCAT-AS-001050 (Manual)	☐	☐
1.57	TCAT-AS-001060 (Manual)	☐	☐
1.58	TCAT-AS-001080 (Manual)	☐	☐
1.59	TCAT-AS-001200 (Manual)	☐	☐
1.60	TCAT-AS-001220 (Manual)	☐	☐
1.61	TCAT-AS-001260 (Manual)	☐	☐
1.61	TCAT-AS-001250 (Manual)	☐	☐
1.63	TCAT-AS-001270 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	TCAT-AS-001280 (Manual)	☐	☐
1.65	TCAT-AS-001320 (Manual)	☐	☐
1.66	TCAT-AS-001430 (Manual)	☐	☐
1.67	TCAT-AS-001460 (Manual)	☐	☐
1.68	TCAT-AS-001470 (Manual)	☐	☐
1.69	TCAT-AS-001560 (Manual)	☐	☐
1.70	TCAT-AS-001590 (Manual)	☐	☐
1.71	TCAT-AS-001591 (Manual)	☐	☐
1.72	TCAT-AS-001592 (Manual)	☐	☐
1.73	TCAT-AS-001640 (Manual)	☐	☐
1.74	TCAT-AS-001660 (Manual)	☐	☐
1.75	TCAT-AS-001670 (Manual)	☐	☐
1.76	TCAT-AS-001680 (Manual)	☐	☐
1.77	TCAT-AS-001690 (Manual)	☐	☐
1.78	TCAT-AS-001700 (Manual)	☐	☐
1.79	TCAT-AS-001710 (Manual)	☐	☐
1.80	TCAT-AS-001720 (Manual)	☐	☐
1.81	TCAT-AS-001730 (Manual)	☐	☐
1.82	TCAT-AS-001731 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 11, 2025	1.0.0	Initial CIS Release