Apache Tomcat Web Server Provisioning and Hardening Checklist

General Information

Name of Individual Performing the Apache Tomcat Web Server Provisioning and Hardening

Last Name	First Name	Middle Name	Title	Date of Review

Additional Information

Department	Division	Office	Immediate Supervisor

Server Information

(1). Hostname of Web Server		Additional Information:
(2). Version | Release Number		
(3). IP Address of Web Server		
(4). Function of Web Server		
(5). Operating System utilized on Web Server		
(6). FIPS Security Category		
(7). Data | Info. Classification Level		

Vulnerability Severity Codes

Severity 1	Vulnerabilities which when exploited lead to immediate superuser access, unauthorized access to a machine, or allow an attacker to bypass security controls.
Severity 2	Vulnerabilities which provide an attacker information with a high probability of allowing unauthorized access to a machine, or to bypass security controls.
Severity 3	Vulnerabilities which grant an attacker information that may possibly lead to the compromise of a machine, or the bypassing of existing security controls
Severity 4	Vulnerabilities which generally degrade the overall security of a system when left unresolved.

Server Configuration Checklist

	Task	Severity Code	Date Completed	Signature
(1).	Ensure that the most updated and vendor supported version of Tomcat is installed.	1		

Additional Information:				
(2).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Unless a documented need exists, disable symbolic linking by ensuring the allowLinking flag is set to false.	1		
Additional Information:				
(3).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Ensure that MIME types for */bin/csh* and */bin/sh* is disabled.	2		
Additional Information:				
(4).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Each interactive program or CGI script should be placed in a specific directory outside the document root, with ACLs reflecting the following: **System Administrator: full** **Web service account: read/execute** **Group (web users): execute** **Other: none**	2		
Additional Information:				
(5).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Each interactive program and CGI script should be owned by a privileged account, and not by the anonymous web user account.	2		
Additional Information:				

(6).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Ensure that no backup copies of scripts or files reside on a production web server.	2		
Additional Information:				
(7).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Verify that none of the server's web content resides in a shared folder.	2		
Additional Information:				
(8).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	With the exception of the Java Development Kit for Java Server Pages applications, ensure that no compilers exist on the production web server.	2		
Additional Information:				
(9).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Ensure that there is at least some limit to the maximum number of HTTP requests by verifying the *maxThreads* value.	2		
Additional Information:				
(10).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	Ensure that the Tomcat process is being run by a non-privileged account.	2		

Note: This is just an introductory preview of this provisioning and hardening checklist.