**CS 305 Module Two Static Testing Summary Template**

**Instructions**

Replace the bracketed text with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

**Run Dependency Check**

A screenshot of a computer

AI-generated content may be incorrect.

**Document Results**

* **hibernate-validator-6.0.18.Final.jar**
  + Provides Hibernate’s Bean Validation (JSR-380) reference implementation.
  + A vulnerability was found in version 6.1.2.Final where error message interpolation allowed the execution of invalid EL expressions. This could enable attackers to bypass input sanitization and introduce malicious content.
* **jackson-databind-2.10.2.jar**
  + A core component for general data-binding in Jackson, built on its streaming API.
  + Versions prior to 2.13.0 are susceptible to Java StackOverflowError and denial-of-service (DoS) through deeply nested object input.
* **log4j-api-2.12.1.jar**
  + Apache Log4j logging API.
  + A critical vulnerability allows remote code execution (RCE) if an attacker can modify the logging configuration to use a malicious JDBC Appender referencing a JNDI URI.
* **logback-core-1.2.3.jar**
  + Core module for the Logback logging framework.
  + In versions 1.2.7 and earlier, attackers with configuration file access could inject malicious content enabling arbitrary code execution via LDAP.
* **snakeyaml-1.25.jar**
  + YAML parser and emitter for Java, based on YAML 1.1.
  + Vulnerable to entity expansion attacks due to unsafe handling of the Alias feature—similar to CVE-2003-1564.
* **spring-aop-5.2.3.RELEASE.jar**
  + Supports aspect-oriented programming (AOP) within Spring applications.
  + Certain versions are vulnerable to specially crafted SpEL expressions that could cause denial-of-service attacks.
* **spring-boot-2.2.4.RELEASE.jar**
  + Framework for simplifying Spring-based applications.
  + Affected by the same SpEL-based DoS vulnerability as Spring AOP and Core in corresponding version ranges.
* **spring-core-5.2.3.RELEASE.jar**
  + Core functionalities for the Spring Framework.
  + Susceptible to SpEL expression abuse leading to denial-of-service, requiring updates for mitigation.
* **tomcat-embed-core-9.0.30.jar**
  + Embedded Tomcat server core module.
  + Documentation incorrectly suggested EncryptInterceptor secures clustering over untrusted networks. However, it does not address all security concerns, particularly those related to DoS.
* **tomcat-embed-websocket-9.0.30.jar**
  + Provides embedded WebSocket support in Tomcat.
  + Shares the same security concerns as the core module regarding insufficient protection when used over untrusted networks.

**Interpreting Results and Recommended Mitigations**

* **hibernate-validator-6.0.18.Final.jar**
  + Upgrade to version **6.0.20.Final** or newer to resolve the EL expression vulnerability.
* **jackson-databind-2.10.2.jar**
  + Mitigate the StackOverflow/DoS risk by upgrading to **version 2.13.0 or later**.
* **log4j-api-2.12.1.jar**
  + Restrict JNDI data source names to the java: protocol and update to a patched version of **Log4j2**.
* **logback-core-1.2.3.jar**
  + Upgrade to **logback version 1.2.8 or later** to address arbitrary code execution vulnerabilities.
* **snakeyaml-1.25.jar**
  + Update to **SnakeYAML 1.26 or newer** to prevent entity expansion vulnerabilities (CVE-2017-18640).
* **spring-aop-5.2.3.RELEASE.jar**
  + Upgrade to **5.2.20+** or **5.3.17+** depending on your current branch.
* **spring-boot-2.2.4.RELEASE.jar**
  + Vulnerability resolved in **v2.2.11.RELEASE or later**.
* **spring-core-5.2.3.RELEASE.jar**
  + Apply the same patching strategy as Spring AOP: upgrade to **5.2.20+** or **5.3.17+**.
* **tomcat-embed-core / tomcat-embed-websocket-9.0.30.jar**
  + For secure clustering over untrusted networks, use a secure alternative such as **VPN tunneling** instead of relying on EncryptInterceptor alone.

Filtering **false positives** from dependency scanning tools is essential. A high number of irrelevant alerts can obscure real threats, leading to delays in patching legitimate issues or overlooking vulnerabilities entirely. Ensuring accurate reporting improves response time and reduces risk in the development cycle.