**Brandon Hobbs**

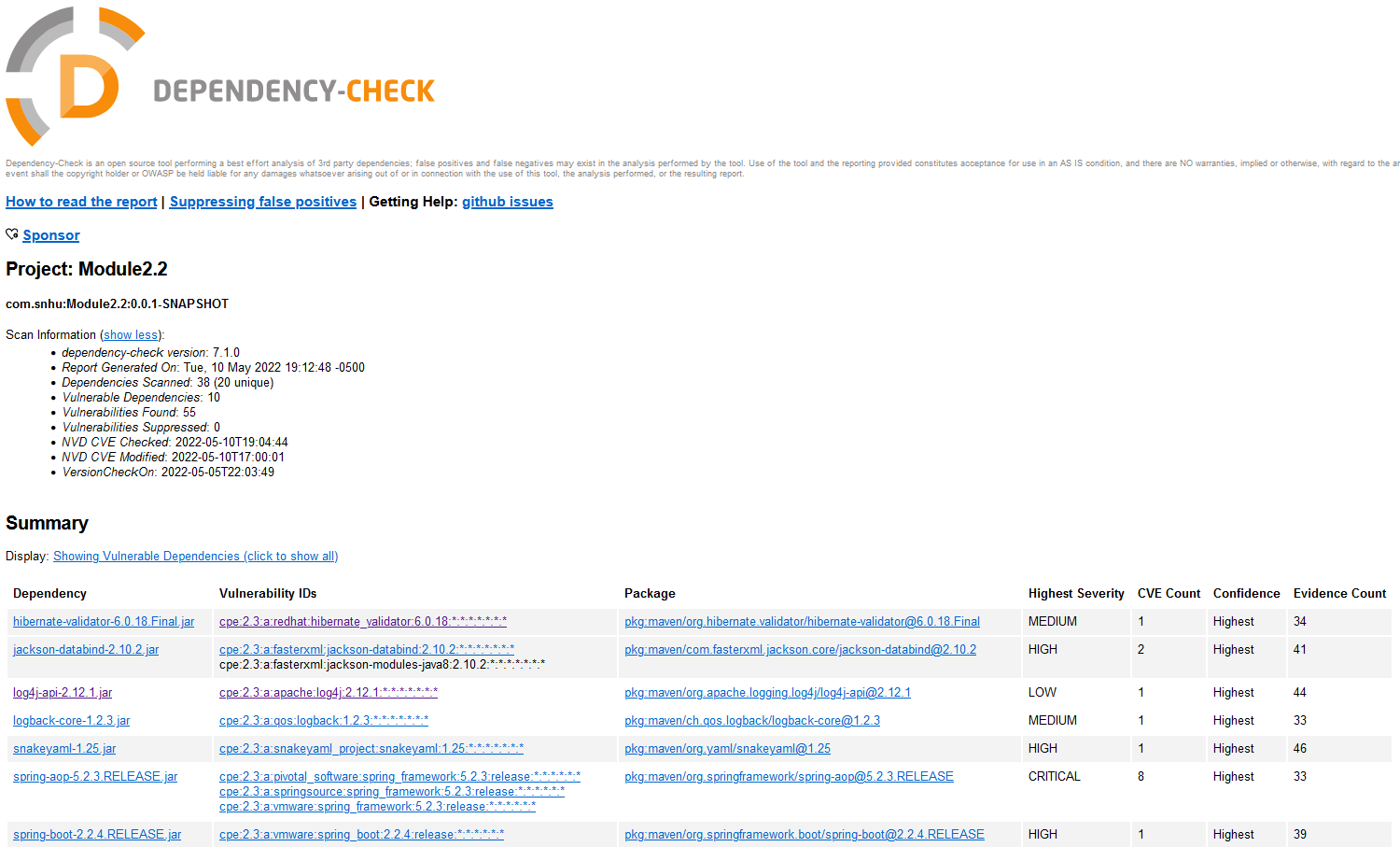
**CS-305**

**May 10, 2022**

**Module2: Static Testing**

### Run Dependency Check

Maven Build Run and Completed May 10, 2022



### Document Results

hibernate-validator-6.0.18.Final.jar

Description: Hibernate's Bean Validation (JSR-380) reference implementation.

License: http://www.apache.org/licenses/LICENSE-2.0.txt

jackson-databind-2.10.2.jar

Description: General data-binding functionality for Jackson: works on core streaming API

License: <http://www.apache.org/licenses/LICENSE-2.0.txt>

log4j-api-2.12.1.jar

Description: The Apache Log4j API

License: <https://www.apache.org/licenses/LICENSE-2.0.txt>

logback-core-1.2.3.jar

Description: logback-core module

License: http://www.eclipse.org/legal/epl-v10.html, <http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html>

snakeyaml-1.25.jar

Description: YAML 1.1 parser and emitter for Java

License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

spring-aop-5.2.3.RELEASE.jar

Description: Spring AOP

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

spring-boot-2.2.4.RELEASE.jar

Description: Spring Boot

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

spring-core-5.2.3.RELEASE.jar

Description: Spring Core

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

tomcat-embed-core-9.0.30.jar

Description: Core Tomcat implementation

License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

tomcat-embed-websocket-9.0.30.jar

Description: Core Tomcat implementation

License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

### Interpret Results

False Positives lead you down a path you do not need to traverse. That is, they are suggesting work that isn’t valuable. Even worse they distract you from actual work that is valuable, i.e., real vulnerabilities. It’s also possible to introduce new bugs, security issues, and possible breaking changes to a code base changing something that was fully functioning and secure!

For this report, I do not see any false positives. All of the CPE seem to correspond to the listed dependency, at least for the dependencies that show a vulnerability – those that are “safe” have been filtered out.

**hibernate-validator-6.0.18.Final.jar**

Hibernate Validator has a flaw in the interpolation processor that “enables invalid EL expressions to be evaluated as if they were valid”. Upgrading to version 6.1.7 would be recommended. This considered to be a severity score of: **medium**.

**jackson-databind-2.10.2.jar**

Jackson Databind has 2 vulnerabilities. One allows for a stack overflow and possible DOS. Upgrading to a newer version (2.13.X) would be suggested. This is considered a severity of: **high**.

The other vulnerability concerns “allow[ing] vulnerability to XML external entity (XXE) attacks”. This is considered another: **high**.

**log4j-api-2.12.1.jar**

log4j was highlighted in one of the largest vulnerabilities (Log4Shell) in the last 6 months. The library version here is 2.12.1 is included in this issue. The official fix was released in 2.15 where more vulnerabilities were discovered and in the subsequent 2.16. log4j 2.17.0 address all the critical vulnerabilities. Severity: **critical**.

**logback-core-1.2.3.jar**

Arbitrary code could be executed from LDAP servers in versions 1.2.7. Upgrading to 1.2.11 is recommended Severity: **medium**.

**snakeyaml-1.25.jar**

The listed vulnerability allows entity expansion during load. The latest version of the library is 1.30 and no vulnerabilities have been listed since v 1.26. Severity: **high**.

**spring-aop-5.2.3.RELEASE.jar**

There are 8 listed vulnerabilities in this library. The vulnerabilities include remote code execution, privilege escalation, malicious log insertion, and DOS. 5.3.X was released to fix vulnerabilities in 5.2.X – upgrade is warranted. Severity: **medium** through **critical**.

**spring-boot-2.2.4.RELEASE.jar**

This issue allows for temporary directory hijacking. Version 2.6.x was released in October of 2021 and an update should be considered. Severity: **high**.

**spring-core-5.2.3.RELEASE.jar**

This library has 8 listed issues. The issues are the same as the 8 issues identified in other parts of the 5.2.3 framework (see spring-aop-5.2.3.RELEASE.jar). 5.3.X was released to fix vulnerabilities in 5.2.X – upgrade is warranted. Severity: **medium** through **critical**.

**tomcat-embed-core-9.0.30.jar**

16 issues, including critical flaws, are identified in this library. Some of the 16 vulnerabilities include: DOS from infinite loops, request smuggling, users being able to view other users’ requests, request leakage, DOS from OutOfMemoryException, vulnerability to high memory usage causing instability. Apache Tomcat is now on version 9.0.63 – given that the issues are critical an update should be considered mandatory. The 16 issues are considered **medium** to **critical**.

**tomcat-embed-websocket-9.0.30.jar**

The same 16 vulnerabilities are listed for this component of the tomcat embedded server as above (see tomcat-embed-core-9.0.30.jar). Apache Tomcat is now on version 9.0.63 – given that the issues are critical an update should be considered mandatory. Severity: **medium** to **critical**.