# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **07/21/2024** | **Sean Lant** |  |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In this report, identify your security vulnerability findings and recommend the next steps to remedy the issues you have found.

* Respond to the five steps outlined below and include your findings.
* Respond using your own words. You may also include images or supporting materials. If you include them, make certain to insert them in the relevant locations in the document.
* Refer to the Project One Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Sean Lant

**1. Interpreting Client Needs**

Determine your client’s needs and potential threats and attacks associated with the company’s application and software security requirements. Consider the following questions regarding how companies protect against external threats based on the scenario information:

* What is the value of secure communications to the company?
* Are there any international transactions that the company produces?
* Are there governmental restrictions on secure communications to consider?
* What external threats might be present now and in the immediate future?
* What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?

When it comes to Artemis Financial, they are a consultant company that specializes in the financial sector. The need for security when it comes to financial data is crucial for maintaining customer trust as well as making sure they comply with government regulations. A big way they do this is by encrypting data that's in transit which makes it harder for data leaks. They do not necessarily state they do international transactions but if they were to engage in international transactions, they would also have to comply with data protection laws to maintain data security. There will be certain regulations that require data protection to be secure for financial institutions to protect against as they are high-value targets. When it comes to external threats some of the easiest ways to gain information are through phishing and social engineering scams that trick employees into revealing sensitive information. Additionally, with financial institutions SQL injections are popular as they can manipulate database queries which could result in thief. When it comes to open-source libraries it's important to regularly update as more outdated libraries are more at risk. Additionally, the use of more modern web frameworks that prioritize security, which so often comes with built-in security features.

**2. Areas of Security**

Refer to the vulnerability assessment process flow diagram. Identify which areas of security apply to Artemis Financial’s software application. Justify your reasoning for why each area is relevant to the software application.

A higher code quality is essential for preventing data exposures as by following secure coding practices vulnerabilities can be avoided, which ensures only authorized users can access specific methods and features. Ensuring code is clean and secure maintains the application by reducing the risk of security flaws. Additionally, the API controls how users interact with the application and specifies which methods are acceptable for accessing data. Securing the API is crucial to prevent unauthorized access and ensure that data exchanges between the application and any third-party systems are safe and dependable. By managing errors properly, we can prevent unauthorized access and privilege escalation. This means avoiding the revelation of sensitive information in error messages and ensuring that exceptions are handled securely, thus minimizing the risk of creating new vulnerabilities. Lastly, Cryptography is crucial for protecting international transactions that involve sensitive customer data. By implementing robust encryption methods, Artemis Financial can ensure that data remains confidential and secure throughout its transmission and storage. This approach not only meets North American security standards but also complies with regulations in other countries, to safeguard information from unauthorized access and leaks.

**3. Manual Review**

Continue working through the vulnerability assessment process flow diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

When it came to the vulnerability assessment process my first focus was on input validation. I checked the POM.XML file from the validator configurations but didn’t find any. Moving on, I reviewed the greeting controller, where it became apparent that input validation was missing. Without any output to test, I couldn’t fully confirm this absence. I then searched for an API and found none in operation. The program was retrieving data through URLs, which is insecure compared to using POST methods. This method exposes data to potential breaches through browser history. Even though the program doesn’t display the data, accepting input via URLs without proper validation is a security risk. Moreover, the lack of a functional API means users don’t have clear guidelines for interacting with the application unless they explore the code themselves. A well-designed RESTful API should provide a clear interaction model for users. Next, I examined cryptographic measures and found no encryption was implemented. Artemis Financial will need to establish robust encryption for both data storage and international transactions to meet global security standards. When checking error handling I noticed that the DocData.java class was lacking in this area, so I contained only basic try-and-catch blocks without additional error management. Lastly, while the code quality was generally high, the absence of an operational API made the application less user-friendly. Additionally, the lack of input validation and the use of URLs for data handling, rather than secure POST methods, poses significant security risks, including potential data leaks.

**4. Static Testing**

Run a dependency check on Artemis Financial’s software application to identify all security vulnerabilities in the code. Record the output from the dependency-check report. Include the following items:

* The names or vulnerability codes of the known vulnerabilities
* A brief description and recommended solutions provided by the dependency-check report
* Any attribution that documents how this vulnerability has been identified or documented previously

### [slf4j-api-1.7.30.jar

**Description:**

The slf4j API

**File Path:** C:\Users\dasj4\.m2\repository\org\slf4j\slf4j-api\1.7.30\slf4j-api-1.7.30.jar  
**MD5:** f8be00da99bc4ab64c79ab1e2be7cb7c  
**SHA1:** b5a4b6d16ab13e34a88fae84c35cd5d68cac922c  
**SHA256:**cdba07964d1bb40a0761485c6b1e8c2f8fd9eb1d19c53928ac0d7f9510105c57  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.slf4j/slf4j-api@1.7.30](https://ossindex.sonatype.org/component/pkg:maven/org.slf4j/slf4j-api@1.7.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**bcprov-jdk15on-1.46.jar**

**Description:**

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.7.

**License:**

Bouncy Castle Licence: http://www.bouncycastle.org/licence.html

**File Path:** C:\Users\dasj4\.m2\repository\org\bouncycastle\bcprov-jdk15on\1.46\bcprov-jdk15on-1.46.jar  
**MD5:** b94e6fef30e871f1b4117232cdc75369  
**SHA1:** 991c96a4e31e6c19e2b9136c8955bd423f2dc4c7  
**SHA256:**a1952237d941ef0b6122ba27b0b58de602de91c714ba3ddd4eef30ba3f5a0a67  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46](https://ossindex.sonatype.org/component/pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Abouncycastle&cpe_product=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api&cpe_version=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api%3A1.46)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

[**CVE-2013-1624**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1624)  suppress

The TLS implementation in the Bouncy Castle Java library before 1.48 and C# library before 1.8 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

CWE-310 Cryptographic Issues  
  
CVSSv2:

* Base Score: MEDIUM (4.0)
* Vector: /AV:N/AC:H/Au:N/C:P/I:P/A:N

References:

* MISC - <http://www.isg.rhul.ac.uk/tls/TLStiming.pdf>
* MLIST - [[oss-security] 20130205 Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations](http://openwall.com/lists/oss-security/2013/02/05/24)
* OSSINDEX - [[CVE-2013-1624] CWE-310](https://ossindex.sonatype.org/vulnerability/CVE-2013-1624?component-type=maven&component-name=org.bouncycastle%2Fbcprov-jdk15on&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)
* REDHAT - [RHSA-2014:0371](http://rhn.redhat.com/errata/RHSA-2014-0371.html)
* REDHAT - [RHSA-2014:0372](http://rhn.redhat.com/errata/RHSA-2014-0372.html)
* SECUNIA - [57716](http://secunia.com/advisories/57716)
* SECUNIA - [57719](http://secunia.com/advisories/57719)

Vulnerable Software & Versions: ([show all](file:///C:\Users\dasj4\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html))

* [cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\*](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api%3A1.46)
* ...

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

**Description:**

Spring Boot

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\boot\spring-boot\2.2.4.RELEASE\spring-boot-2.2.4.RELEASE.jar  
**MD5:** 24de0cfd8ea74b903b562b43cbc5eb13  
**SHA1:** 225a4fd31156c254e3bb92adb42ee8c6de812714  
**SHA256:**176befc7b90e8498f44e21994a70d69ba360ef1e858ff3cea8282e802372daf2  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Related Dependencies**

**Identifiers**

* [pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_boot&cpe_version=cpe%3A%2F%3Avmware%3Aspring_boot%3A2.2.4)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

[**CVE-2022-27772**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772)  suppress

spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer

CWE-668 Exposure of Resource to Wrong Sphere  
  
CVSSv2:

* Base Score: MEDIUM (4.6)
* Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:

* Base Score: HIGH (7.8)
* Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:

* MISC - <https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85>
* OSSINDEX - [[CVE-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere](https://ossindex.sonatype.org/vulnerability/CVE-2022-27772?component-type=maven&component-name=org.springframework.boot%2Fspring-boot&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions:

* [cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.2.11](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Avmware%3Aspring_boot)

**log4j-api-2.12.1.jar**

**Description:**

The Apache Log4j API

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\apache\logging\log4j\log4j-api\2.12.1\log4j-api-2.12.1.jar  
**MD5:** 4a6f276d4fb426c8d489343c0325bb75  
**SHA1:** a55e6d987f50a515c9260b0451b4fa217dc539cb  
**SHA256:**429534d03bdb728879ab551d469e26f6f7ff4c8a8627f59ac68ab6ef26063515  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Related Dependencies**

**Identifiers**

* [pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1](https://ossindex.sonatype.org/component/pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Alog4j&cpe_version=cpe%3A%2F%3Aapache%3Alog4j%3A2.12.1)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

[**CVE-2020-9488**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9488)  suppress

Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1

CWE-295 Improper Certificate Validation  
  
CVSSv2:

* Base Score: MEDIUM (4.3)
* Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3:

* Base Score: LOW (3.7)
* Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:

* - [[db-torque-dev] 20200715 Build failed in Jenkins: Torque4-trunk #685](https://lists.apache.org/thread.html/r393943de452406f0f6f4b3def9f8d3c071f96323c1f6ed1a098f7fe4%40%3Ctorque-dev.db.apache.org%3E)
* - [[db-torque-dev] 20210127 Re: Items for our (delayed) quarterly report to the board?](https://lists.apache.org/thread.html/rc2dbc4633a6eea1fcbce6831876cfa17b73759a98c65326d1896cb1a%40%3Ctorque-dev.db.apache.org%3E)
* - [[db-torque-dev] 20210128 Antwort: Re: Items for our (delayed) quarterly report to the board?](https://lists.apache.org/thread.html/rd5d58088812cf8e677d99b07f73c654014c524c94e7fedbdee047604%40%3Ctorque-dev.db.apache.org%3E)
* - [[flink-issues] 20210510 [GitHub] [flink] zentol opened a new pull request #15879: [FLINK-22407][build] Bump log4j to 2.24.1](https://lists.apache.org/thread.html/r45916179811a32cbaa500f972de9098e6ee80ee81c7f134fce83e03a%40%3Cissues.flink.apache.org%3E)
* - [[hive-dev] 20201207 [jira] [Created] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r4db540cafc5d7232c62e076051ef661d37d345015b2e59b3f81a932f%40%3Cdev.hive.apache.org%3E)
* - [[hive-dev] 20210216 [jira] [Created] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r4d5dc9f3520071338d9ebc26f9f158a43ae28a91923d176b550a807b%40%3Cdev.hive.apache.org%3E)
* - [[hive-issues] 20201207 [jira] [Assigned] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/ra632b329b2ae2324fabbad5da204c4ec2e171ff60348ec4ba698fd40%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20201207 [jira] [Updated] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r4ed1f49616a8603832d378cb9d13e7a8b9b27972bb46d946ccd8491f%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20201207 [jira] [Work started] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r1fc73f0e16ec2fa249d3ad39a5194afb9cc5afb4c023dc0bab5a5881%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20201208 [jira] [Updated] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r65578f3761a89bc164e8964acd5d913b9f8fd997967b195a89a97ca3%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20201208 [jira] [Work logged] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r9776e71e3c67c5d13a91c1eba0dc025b48b802eb7561cc6956d6961c%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20210125 [jira] [Work logged] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r3d1d00441c55144a4013adda74b051ae7864128ebcfb6ee9721a2eb3%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20210209 [jira] [Resolved] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r33864a0fc171c1c4bf680645ebb6d4f8057899ab294a43e1e4fe9d04%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20210216 [jira] [Assigned] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r5a68258e5ab12532dc179edae3d6e87037fa3b50ab9d63a90c432507%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20210216 [jira] [Resolved] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/r22a56beb76dd8cf18e24fda9072f1e05990f49d6439662d3782a392f%40%3Cissues.hive.apache.org%3E)
* - [[hive-issues] 20210218 [jira] [Updated] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488](https://lists.apache.org/thread.html/ra051e07a0eea4943fa104247e69596f094951f51512d42c924e86c75%40%3Cissues.hive.apache.org%3E)
* - [[kafka-dev] 20200514 [jira] [Created] (KAFKA-9996) upgrade zookeeper to 3.5.8 to address security vulnerabilities](https://lists.apache.org/thread.html/r7e5c10534ed06bf805473ac85e8412fe3908a8fa4cabf5027bf11220%40%3Cdev.kafka.apache.org%3E)
* - [[kafka-dev] 20200514 [jira] [Created] (KAFKA-9997) upgrade log4j lib to address CVE-2020-9488](https://lists.apache.org/thread.html/rf1c2a81a08034c688b8f15cf58a4cfab322d00002ca46d20133bee20%40%3Cdev.kafka.apache.org%3E)
* - [[kafka-jira] 20200514 [jira] [Created] (KAFKA-9996) upgrade zookeeper to 3.5.8 to address security vulnerabilities](https://lists.apache.org/thread.html/r8e96c340004b7898cad3204ea51280ef6e4b553a684e1452bf1b18b1%40%3Cjira.kafka.apache.org%3E)
* - [[kafka-jira] 20200514 [jira] [Created] (KAFKA-9997) upgrade log4j lib to address CVE-2020-9488](https://lists.apache.org/thread.html/r0a2699f724156a558afd1abb6c044fb9132caa66dce861b82699722a%40%3Cjira.kafka.apache.org%3E)
* - [[kafka-jira] 20200515 [jira] [Commented] (KAFKA-9997) upgrade log4j lib to address CVE-2020-9488](https://lists.apache.org/thread.html/r48bcd06049c1779ef709564544c3d8a32ae6ee5c3b7281a606ac4463%40%3Cjira.kafka.apache.org%3E)
* - [[kafka-users] 20210617 vulnerabilities](https://lists.apache.org/thread.html/r2721aba31a8562639c4b937150897e24f78f747cdbda8641c0f659fe%40%3Cusers.kafka.apache.org%3E)
* - [[mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar](https://lists.apache.org/thread.html/rf9fa47ab66495c78bb4120b0754dd9531ca2ff0430f6685ac9b07772%40%3Cdev.mina.apache.org%3E)
* - [[pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list](https://lists.apache.org/thread.html/rd0e44e8ef71eeaaa3cf3d1b8b41eb25894372e2995ec908ce7624d26%40%3Ccommits.pulsar.apache.org%3E)
* - [[zookeeper-commits] 20200504 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488](https://lists.apache.org/thread.html/rec34b1cccf907898e7cb36051ffac3ccf1ea89d0b261a2a3b3fb267f%40%3Ccommits.zookeeper.apache.org%3E)
* - [[zookeeper-commits] 20200504 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488](https://lists.apache.org/thread.html/r48efc7cb5aeb4e1f67aaa06fb4b5479a5635d12f07d0b93fc2d08809%40%3Ccommits.zookeeper.apache.org%3E)
* - [[zookeeper-commits] 20200504 [zookeeper] branch master updated: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488](https://lists.apache.org/thread.html/rbc45eb0f53fd6242af3e666c2189464f848a851d408289840cecc6e3%40%3Ccommits.zookeeper.apache.org%3E)
* - [[zookeeper-dev] 20200504 [jira] [Created] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488](https://lists.apache.org/thread.html/r2f209d271349bafd91537a558a279c08ebcff8fa3e547357d58833e6%40%3Cdev.zookeeper.apache.org%3E)
* - [[zookeeper-dev] 20200504 log4j SmtpAppender related CVE](https://lists.apache.org/thread.html/r0df3d7a5acb98c57e64ab9266aa21eeee1d9b399addb96f9cf1cbe05%40%3Cdev.zookeeper.apache.org%3E)
* - [[zookeeper-issues] 20200504 [jira] [Assigned] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488](https://lists.apache.org/thread.html/rd8e87c4d69df335d0ba7d815b63be8bd8a6352f429765c52eb07ddac%40%3Cissues.zookeeper.apache.org%3E)
* - [[zookeeper-issues] 20200504 [jira] [Commented] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488](https://lists.apache.org/thread.html/r4285398e5585a0456d3d9db021a4fce6e6fcf3ec027dfa13a450ec98%40%3Cissues.zookeeper.apache.org%3E)
* - [[zookeeper-issues] 20200504 [jira] [Created] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488](https://lists.apache.org/thread.html/r8c001b9a95c0bbec06f4457721edd94935a55932e64b82cc5582b846%40%3Cissues.zookeeper.apache.org%3E)
* - [[zookeeper-issues] 20200504 [jira] [Resolved] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488](https://lists.apache.org/thread.html/rd55f65c6822ff235eda435d31488cfbb9aa7055cdf47481ebee777cc%40%3Cissues.zookeeper.apache.org%3E)
* - [[zookeeper-issues] 20200504 [jira] [Updated] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488](https://lists.apache.org/thread.html/r9a79175c393d14d760a0ae3731b4a873230a16ef321aa9ca48a810cd%40%3Cissues.zookeeper.apache.org%3E)
* - [[zookeeper-notifications] 20200504 Build failed in Jenkins: zookeeper-master-maven-owasp #489](https://lists.apache.org/thread.html/r7641ee788e1eb1be4bb206a7d15f8a64ec6ef23e5ec6132d5a567695%40%3Cnotifications.zookeeper.apache.org%3E)
* - [[zookeeper-notifications] 20200504 [GitHub] [zookeeper] symat commented on pull request #1346: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488](https://lists.apache.org/thread.html/rc6b81c013618d1de1b5d6b8c1088aaf87b4bacc10c2371f15a566701%40%3Cnotifications.zookeeper.apache.org%3E)
* - [[zookeeper-notifications] 20200504 [GitHub] [zookeeper] symat opened a new pull request #1346: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488](https://lists.apache.org/thread.html/r7e739f2961753af95e2a3a637828fb88bfca68e5d6b0221d483a9ee5%40%3Cnotifications.zookeeper.apache.org%3E)
* - <https://lists.apache.org/thread.html/rbc7642b9800249553f13457e46b813bea1aec99d2bc9106510e00ff3%40%3Ctorque-dev.db.apache.org%3E>
* - <https://lists.apache.org/thread.html/re024d86dffa72ad800f2848d0c77ed93f0b78ee808350b477a6ed987%40%3Cgitbox.hive.apache.org%3E>
* CONFIRM - <https://issues.apache.org/jira/browse/LOG4J2-2819>
* CONFIRM - <https://security.netapp.com/advisory/ntap-20200504-0003/>
* DEBIAN - [DSA-5020](https://www.debian.org/security/2021/dsa-5020)
* MISC - <https://www.oracle.com/security-alerts/cpuApr2021.html>
* MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
* MISC - <https://www.oracle.com/security-alerts/cpujan2021.html>
* MISC - <https://www.oracle.com/security-alerts/cpujul2020.html>
* MISC - <https://www.oracle.com/security-alerts/cpuoct2020.html>
* MISC - <https://www.oracle.com/security-alerts/cpuoct2021.html>
* MLIST - [[debian-lts-announce] 20211226 [SECURITY] [DLA 2852-1] apache-log4j2 security update](https://lists.debian.org/debian-lts-announce/2021/12/msg00017.html)

Vulnerable Software & Versions: ([show all](file:///C:\Users\dasj4\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html))

* [cpe:2.3:a:apache:log4j:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 2.4; versions up to (excluding) 2.12.3](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Aapache%3Alog4j)
* ...

**jul-to-slf4j-1.7.30.jar**

**Description:**

JUL to SLF4J bridge

**File Path:** C:\Users\dasj4\.m2\repository\org\slf4j\jul-to-slf4j\1.7.30\jul-to-slf4j-1.7.30.jar  
**MD5:** f2c78cb93d70dc5dea0c50f36ace09c1  
**SHA1:** d58bebff8cbf70ff52b59208586095f467656c30  
**SHA256:**bbcbfdaa72572255c4f85207a9bfdb24358dc993e41252331bd4d0913e4988b9  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.slf4j/jul-to-slf4j@1.7.30](https://ossindex.sonatype.org/component/pkg:maven/org.slf4j/jul-to-slf4j@1.7.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**jakarta.annotation-api-1.3.5.jar**

**Description:**

Jakarta Annotations API

**License:**

EPL 2.0: http://www.eclipse.org/legal/epl-2.0

GPL2 w/ CPE: https://www.gnu.org/software/classpath/license.html

**File Path:** C:\Users\dasj4\.m2\repository\jakarta\annotation\jakarta.annotation-api\1.3.5\jakarta.annotation-api-1.3.5.jar  
**MD5:** 8b165cf58df5f8c2a222f637c0a07c97  
**SHA1:** 59eb84ee0d616332ff44aba065f3888cf002cd2d  
**SHA256:**85fb03fc054cdf4efca8efd9b6712bbb418e1ab98241c4539c8585bbc23e1b8a  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/jakarta.annotation/jakarta.annotation-api@1.3.5](https://ossindex.sonatype.org/component/pkg:maven/jakarta.annotation/jakarta.annotation-api@1.3.5?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**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

**File Path:** C:\Users\dasj4\.m2\repository\org\yaml\snakeyaml\1.25\snakeyaml-1.25.jar  
**MD5:** 6f7d5b8f596047aae07a3bf6f23a0bf2  
**SHA1:** 8b6e01ef661d8378ae6dd7b511a7f2a33fae1421  
**SHA256:**b50ef33187e7dc922b26dbe4dd0fdb3a9cf349e75a08b95269901548eee546eb  
**Referenced In Project/Scope:**rest-service:runtime

**Evidence**

**Identifiers**

* [pkg:maven/org.yaml/snakeyaml@1.25](https://ossindex.sonatype.org/component/pkg:maven/org.yaml/snakeyaml@1.25?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Asnakeyaml_project&cpe_product=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml&cpe_version=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml%3A1.25)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:yaml\_project:yaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Ayaml_project&cpe_product=cpe%3A%2F%3Ayaml_project%3Ayaml&cpe_version=cpe%3A%2F%3Ayaml_project%3Ayaml%3A1.25)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

[**CVE-2017-18640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640)  suppress

The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')  
  
CVSSv2:

* Base Score: MEDIUM (5.0)
* Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:

* Base Score: HIGH (7.5)
* Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:

* - [FEDORA-2020-23012fafbc](https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/PTVJC54XGX26UJVVYCXZ7D25X3R5T2G6/)
* - [FEDORA-2020-599514b47e](https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/CKN7VGIKTYBCAKYBRG55QHXAY5UDZ7HA/)
* - [[atlas-commits] 20200915 [atlas] branch master updated: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640 (#110)](https://lists.apache.org/thread.html/rce5c93bba6e815fb62ad38e28ca1943b3019af1eddeb06507ad4e11a%40%3Ccommits.atlas.apache.org%3E)
* - [[atlas-commits] 20200916 [atlas] 02/02: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640 (#110)](https://lists.apache.org/thread.html/r1058e7646988394de6a3fd0857ea9b1ee0de14d7bb28fee5ff782457%40%3Ccommits.atlas.apache.org%3E)
* - [[atlas-dev] 20200907 [GitHub] [atlas] crazylab closed pull request #109: Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/r6d54c2da792c74cc14b9b7665ea89e144c9e238ed478d37fd56292e6%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200907 [GitHub] [atlas] crazylab opened a new pull request #109: Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/r1dfac8b6a7097bcb4979402bbb6e2f8c36d0d9001e3018717eb22b7e%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200907 [GitHub] [atlas] crazylab opened a new pull request #110: Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/r2a5b84fdf59042dc398497e914b5bb1aed77328320b1438144ae1953%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200914 [GitHub] [atlas] nixonrodrigues commented on pull request #110: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/r28c9009a48d52cf448f8b02cd823da0f8601d2dff4d66f387a35f1e0%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200914 [jira] [Created] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/rb7b28ac741e32dd5edb2c22485d635275bead7290b056ee56baf8ce0%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200914 [jira] [Updated] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/re791a854001ec1f79cd4f47328b270e7a1d9d7056debb8f16d962722%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200915 [GitHub] [atlas] nixonrodrigues merged pull request #110: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/r5510f0125ba409fc1cabd098ab8b457741e5fa314cbd0e61e4339422%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200915 [jira] [Commented] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/r2db207a2431a5e9e95e899858ab1f5eabd9bcc790a6ca7193ae07e94%40%3Cdev.atlas.apache.org%3E)
* - [[atlas-dev] 20200916 [jira] [Commented] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640](https://lists.apache.org/thread.html/re851bbfbedd47c690b6e01942acb98ee08bd00df1a94910b905bc8cd%40%3Cdev.atlas.apache.org%3E)
* - [[cassandra-commits] 20200930 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/reb1751562ee5146d3aca654a2df76a2c13d8036645ce69946f9c219e%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20200930 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/r1ffce2ed3017e9964f03ad2c539d69e49144fc8e9bf772d641612f98%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20200930 [jira] [Created] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/r56805265475919252ba7fc10123f15b91097f3009bae86476624ca25%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20200930 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/rbaa1f513d903c89a08267c91d86811fa5bcc82e0596b6142c5cea7ea%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201001 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/rc3211c71f7e0973a1825d1988a3921288c06cd9d793eae97ecd34948%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201002 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/recfe569f4f260328b0036f1c82b2956e864d519ab941a5e75d0d832d%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201002 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/r55d807f31e64a080c54455897c20b1667ec792e5915132c7b7750533%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201007 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/r1703a402f30c8a2ee409f8c6f393e95a63f8c952cc9ee5bf9dd586dc%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201007 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/rf95bebee6dfcc55067cebe8482bd31e6f481d9f74ba8e03f860c3ec7%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201009 [cassandra] branch trunk updated: Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/rb5c33d0069c927fae16084f0605895b98d231d7c48527bcb822ac48c%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201009 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/r191ceadb1b883357384981848dfa5235cb02a90070c553afbaf9b3d9%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201009 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/r20350031c60a77b45e0eded33e9b3e9cb0cbfc5e24e1c63bf264df12%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-commits] 20201009 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix](https://lists.apache.org/thread.html/rd582c64f66c354240290072f340505f5d026ca944ec417226bb0272e%40%3Ccommits.cassandra.apache.org%3E)
* - [[cassandra-pr] 20200907 [GitHub] [cassandra] crazylab opened a new pull request #736: Upgrade to a snakeyaml version without CVE](https://lists.apache.org/thread.html/rb0e033d5ec8233360203431ad96580cf2ec56f47d9a425d894e279c2%40%3Cpr.cassandra.apache.org%3E)
* - [[hadoop-common-commits] 20201028 [hadoop] branch branch-3.3 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.](https://lists.apache.org/thread.html/rcb2a7037366c58bac6aec6ce3df843a11ef97ae4eb049f05f410eaa5%40%3Ccommon-commits.hadoop.apache.org%3E)
* - [[hadoop-common-commits] 20201028 [hadoop] branch trunk updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.](https://lists.apache.org/thread.html/r1aab47b48a757c70e40fc0bcb1fcf1a3951afa6a17aee7cd66cf79f8%40%3Ccommon-commits.hadoop.apache.org%3E)
* - [[hadoop-common-commits] 20211008 [hadoop] branch branch-3.2 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.](https://lists.apache.org/thread.html/rdd34c0479587e32a656d976649409487d51ca0d296b3e26b6b89c3f5%40%3Ccommon-commits.hadoop.apache.org%3E)
* - [[hadoop-common-commits] 20211008 [hadoop] branch branch-3.2.3 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.](https://lists.apache.org/thread.html/rfe0aab6c3bebbd9cbfdedb65ff3fdf420714bcb8acdfd346077e1263%40%3Ccommon-commits.hadoop.apache.org%3E)
* - [[hadoop-common-dev] 20200830 [jira] [Created] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/rb34d8d3269ad47a1400f5a1a2d8310e13a80b6576ebd7f512144198d%40%3Ccommon-dev.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20200830 [jira] [Created] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r643ba53f002ae59068f9352fe1d82e1b6f375387ffb776f13efe8fda%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20200830 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r8464b6ec951aace8c807bac9ea526d4f9e3116aa16d38be06f7c6524%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20200831 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r72a3588d62b2de1361dc9648f5d355385735e47f7ba49d089b0e680d%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20200909 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r154090b871cf96d985b90864442d84eb027c72c94bc3f0a5727ba2d1%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20201026 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/rcb4b61dbe2ed1c7a88781a9aff5a9e7342cc7ed026aec0418ee67596%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20201027 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/raebd2019b3da8c2f90f31e8b203b45353f78770ca93bfe5376f5532e%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20201028 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r4d7f37da1bc2df90a5a0f56eb7629b5ea131bfe11eeeb4b4c193f64a%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20201028 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r22ac2aa053b7d9c6b75a49db78125c9316499668d0f4a044f3402e2f%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20211006 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r16ae4e529401b75a1f5aa462b272b31bf2a108236f882f06fddc14bc%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20211008 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r465d2553a31265b042cf5457ef649b71e0722ab89b6ea94a5d59529b%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[hadoop-common-issues] 20211008 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640](https://lists.apache.org/thread.html/r182e9cf6f3fb22b9be0cac4ff0685199741d2ab6e9a4e27a3693c224%40%3Ccommon-issues.hadoop.apache.org%3E)
* - [[kafka-users] 20210617 vulnerabilities](https://lists.apache.org/thread.html/r2721aba31a8562639c4b937150897e24f78f747cdbda8641c0f659fe%40%3Cusers.kafka.apache.org%3E)
* - [[phoenix-dev] 20210419 [GitHub] [phoenix-omid] richardantal opened a new pull request #93: OMID-207 Upgrade to snakeyaml 1.26 due to CVE-2017-18640](https://lists.apache.org/thread.html/r7ce3de03facf7e7f3e24fc25d26d555818519dafdb20f29398a3414b%40%3Cdev.phoenix.apache.org%3E)
* - [[phoenix-dev] 20210419 [jira] [Created] (OMID-207) Upgrade to snakeyaml 1.26 due to CVE-2017-18640](https://lists.apache.org/thread.html/r436988d2cfe8a770ae361c82b181c5b2bf48a249bad84d8a55a3b46e%40%3Cdev.phoenix.apache.org%3E)
* - [[pulsar-commits] 20200830 [GitHub] [pulsar] codelipenghui commented on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26](https://lists.apache.org/thread.html/r8b57c57cffa01e418868a3c7535b987635ff1fb5ab534203bfa2d64a%40%3Ccommits.pulsar.apache.org%3E)
* - [[pulsar-commits] 20200831 [GitHub] [pulsar] wolfstudy commented on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26](https://lists.apache.org/thread.html/r6c91e52b3cc9f4e64afe0f34f20507143fd1f756d12681a56a9b38da%40%3Ccommits.pulsar.apache.org%3E)
* - [[pulsar-commits] 20200831 [GitHub] [pulsar] wolfstudy edited a comment on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26](https://lists.apache.org/thread.html/r2b05744c0c2867daa5d1a96832965b7d6220328b0ead06c22a6e7854%40%3Ccommits.pulsar.apache.org%3E)
* - [[pulsar-commits] 20200907 [GitHub] [pulsar] jiazhai closed issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26](https://lists.apache.org/thread.html/r666f29a7d0e1f98fa1425ca01efcfa86e6e3856e01d300828aa7c6ea%40%3Ccommits.pulsar.apache.org%3E)
* - <https://lists.apache.org/thread.html/r4c682fb8cf69dd14162439656a6ebdf42ea6ad0e4edba95907ea3f14%40%3Ccommits.servicecomb.apache.org%3E>
* - <https://lists.apache.org/thread.html/r900e020760c89f082df1c6e0d46320eba721e4e47bb9eb521e68cd95%40%3Ccommits.servicecomb.apache.org%3E>
* GENTOO - [GLSA-202305-28](https://security.gentoo.org/glsa/202305-28)
* MISC - <https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion>
* MISC - <https://bitbucket.org/asomov/snakeyaml/wiki/Billion%20laughs%20attack>
* MISC - <https://bitbucket.org/snakeyaml/snakeyaml/issues/377>
* MISC - <https://bitbucket.org/snakeyaml/snakeyaml/wiki/Changes>
* MISC - <https://mvnrepository.com/artifact/org.yaml/snakeyaml/1.25/usages>
* MISC - <https://www.oracle.com/security-alerts/cpuApr2021.html>
* OSSINDEX - [[CVE-2017-18640] CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')](https://ossindex.sonatype.org/vulnerability/CVE-2017-18640?component-type=maven&component-name=org.yaml%2Fsnakeyaml&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions: ([show all](file:///C:\Users\dasj4\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html))

* [cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.26](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Asnakeyaml_project%3Asnakeyaml)
* ...

**jackson-annotations-2.10.2.jar**

**Description:**

Core annotations used for value types, used by Jackson data binding package.

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\com\fasterxml\jackson\core\jackson-annotations\2.10.2\jackson-annotations-2.10.2.jar  
**MD5:** d9e46501509b1751d64c495ab088a6cf  
**SHA1:** 3a13b6105946541b8d4181a0506355b5fae63260  
**SHA256:**8c3cba89bf3e03b35a0e6f892c2eb17ed8fdde2e214c3a4c18703d63796bae46  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/com.fasterxml.jackson.core/jackson-annotations@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-annotations@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**jackson-core-2.10.2.jar**

**Description:**

Core Jackson processing abstractions (aka Streaming API), implementation for JSON

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\com\fasterxml\jackson\core\jackson-core\2.10.2\jackson-core-2.10.2.jar  
**MD5:** 5514a46e38331f8c8262ea63bf36483e  
**SHA1:** 73d4322a6bda684f676a2b5fe918361c4e5c7cca  
**SHA256:**4c41f22a48f6ebb28752baeb6d25bf09ba4ff0ad8bfb82650dde448928b9da4f  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**jackson-datatype-jdk8-2.10.2.jar**

**Description:**

Add-on module for Jackson (http://jackson.codehaus.org) to support

JDK 8 data types.

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\com\fasterxml\jackson\datatype\jackson-datatype-jdk8\2.10.2\jackson-datatype-jdk8-2.10.2.jar  
**MD5:** f4fb260e66b9829d37ecd81918c0bcb3  
**SHA1:** dca8c8ab85eaabefe021e2f1ac777f3a6b16a3cb  
**SHA256:**e69a1ec4ffe6f13b2a035c0c13d77b1b08fdc9d3e1f606b69e74c4b2efc89197  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Related Dependencies**

**Identifiers**

* [pkg:maven/com.fasterxml.jackson.datatype/jackson-datatype-jdk8@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.datatype/jackson-datatype-jdk8@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\*  (*Confidence*:Low)  suppress

**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

**File Path:** C:\Users\dasj4\.m2\repository\org\apache\tomcat\embed\tomcat-embed-core\9.0.30\tomcat-embed-core-9.0.30.jar  
**MD5:** f9e49f66756f133157f19e617af26ffe  
**SHA1:** ad32909314fe2ba02cec036434c0addd19bcc580  
**SHA256:**b1415eecbc9f14e3745c1bfd41512a1b8e1af1332a7beaed4be30b2e0ba7b330  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Related Dependencies**

**Identifiers**

* [pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

[**CVE-2019-17569**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)  suppress

The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')  
  
CVSSv2:

* Base Score: MEDIUM (5.8)
* Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3:

* Base Score: MEDIUM (4.8)
* Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

References:

* - [[tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities](https://lists.apache.org/thread.html/rc31cbabb46cdc58bbdd8519a8f64b6236b2635a3922bbeba0f0e3743%40%3Ccommits.tomee.apache.org%3E)
* - [[tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities](https://lists.apache.org/thread.html/r7bc994c965a34876bd94d5ff15b4e1e30b6220a15eb9b47c81915b78%40%3Ccommits.tomee.apache.org%3E)
* CONFIRM - <https://security.netapp.com/advisory/ntap-20200327-0005/>
* DEBIAN - [DSA-4673](https://www.debian.org/security/2020/dsa-4673)
* DEBIAN - [DSA-4680](https://www.debian.org/security/2020/dsa-4680)
* MISC - <https://www.oracle.com/security-alerts/cpujan2021.html>
* MISC - <https://www.oracle.com/security-alerts/cpujul2020.html>
* MISC - <https://www.oracle.com/security-alerts/cpuoct2020.html>
* MLIST - [[debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update](https://lists.debian.org/debian-lts-announce/2020/03/msg00006.html)
* MLIST - [[tomcat-announce] 20200224 [SECURITY] CVE-2019-17569 HTTP Request Smuggling](https://lists.apache.org/thread.html/r88def002c5c78534674ca67472e035099fbe088813d50062094a1390%40%3Cannounce.tomcat.apache.org%3E)
* SUSE - [openSUSE-SU-2020:0345](http://lists.opensuse.org/opensuse-security-announce/2020-03/msg00025.html)

Vulnerable Software & Versions: ([show all](file:///C:\Users\dasj4\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html))

* [cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.28; versions up to (including) 9.0.30](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Aapache%3Atomcat)
* ...

[**CVE-2020-11996**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996)  suppress

A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.

NVD-CWE-noinfo  
  
CVSSv2:

* Base Score: MEDIUM (5.0)
* Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:

* Base Score: HIGH (7.5)
* Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:

* - [[ofbiz-commits] 20200628 [ofbiz-framework] branch release17.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)](https://lists.apache.org/thread.html/r93ca628ef3a4530dfe5ac49fddc795f0920a4b2a408b57a30926a42b%40%3Ccommits.ofbiz.apache.org%3E)
* - [[ofbiz-commits] 20200628 [ofbiz-framework] branch release18.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)](https://lists.apache.org/thread.html/r74f5a8204efe574cbfcd95b2a16236fe95beb45c4d9fee3dc789dca9%40%3Ccommits.ofbiz.apache.org%3E)
* - [[ofbiz-commits] 20200628 [ofbiz-framework] branch trunk updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)](https://lists.apache.org/thread.html/r8f3d416c193bc9384a8a7dd368623d441f5fcaff1057115008100561%40%3Ccommits.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/rb4ee49ecc4c59620ffd5e66e84a17e526c2c3cfa95d0cd682d90d338%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/rea65d6ef2e45dd1c45faae83922042732866c7b88fa109b76c83db52%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200628 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/rc80b96b4b96618b2b7461cb90664a428cfd6605eea9f74e51b792542%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/r8f7484589454638af527182ae55ef5b628ba00c05c5b11887c922fb1%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/rb820f1a2a02bf07414be12c653c2ab5321fd87b9bf6c5e635c53ff4b%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/ra7092f7492569b39b04ec0decf52628ba86c51f15efb38f5853e2760%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200701 [jira] [Reopened] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/r9ad911fe49450ed9405827af0e7a74104041081ff91864b1f2546bbd%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200703 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/r6c29801370a36c1a5159679269777ad0c73276d3015b8bbefea66e5c%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200703 [jira] [Comment Edited] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/ref0339792ac6dac1dba83c071a727ad72380899bde60f6aaad4031b9%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20200703 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/r3ea96d8f36dd404acce83df8aeb22a9e807d6c13ca9c5dec72f872cd%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[ofbiz-notifications] 20210301 [jira] [Updated] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)](https://lists.apache.org/thread.html/r5a4f80a6acc6607d61dae424b643b594c6188dd4e1eff04705c10db2%40%3Cnotifications.ofbiz.apache.org%3E)
* - [[tomcat-users] 20201008 Is Tomcat7 supports HTTP2](https://lists.apache.org/thread.html/r2529016c311ce9485e6f173446d469600fdfbb94dccadfcd9dfdac79%40%3Cusers.tomcat.apache.org%3E)
* CONFIRM - <https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E>
* CONFIRM - <https://security.netapp.com/advisory/ntap-20200709-0002/>
* DEBIAN - [DSA-4727](https://www.debian.org/security/2020/dsa-4727)
* MISC - <https://www.oracle.com/security-alerts/cpujan2021.html>
* MISC - <https://www.oracle.com/security-alerts/cpuoct2020.html>
* MLIST - [[debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update](https://lists.debian.org/debian-lts-announce/2020/07/msg00010.html)
* SUSE - [openSUSE-SU-2020:1051](http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00064.html)
* SUSE - [openSUSE-SU-2020:1063](http://lists.opensuse.org/opensuse-security-announce/2020-07/msg00072.html)
* UBUNTU - [USN-4596-1](https://usn.ubuntu.com/4596-1/)

Vulnerable Software & Versions: ([show all](file:///C:\Users\dasj4\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html))

* [cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.35](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Aapache%3Atomcat)
* ...

**tomcat-embed-el-9.0.30.jar**

**Description:**

Core Tomcat implementation

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\apache\tomcat\embed\tomcat-embed-el\9.0.30\tomcat-embed-el-9.0.30.jar  
**MD5:** f108adf17d4ea57b215a044e5204bfd1  
**SHA1:** 406e0c7cc45204c0f81853d73e8cfedfa4e00945  
**SHA256:**76255aed732a16de40eb1f48fc3c5350eb368d1a80f58a3a0a46170d149fe7eb  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.apache.tomcat.embed/tomcat-embed-el@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-el@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**jakarta.validation-api-2.0.2.jar**

**Description:**

Jakarta Bean Validation API

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\jakarta\validation\jakarta.validation-api\2.0.2\jakarta.validation-api-2.0.2.jar  
**MD5:** 77501d529c1928c9bac2500cc9f93fb0  
**SHA1:** 5eacc6522521f7eacb081f95cee1e231648461e7  
**SHA256:**b42d42428f3d922c892a909fa043287d577c0c5b165ad9b7d568cebf87fc9ea4  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/jakarta.validation/jakarta.validation-api@2.0.2](https://ossindex.sonatype.org/component/pkg:maven/jakarta.validation/jakarta.validation-api@2.0.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**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>

**File Path:** C:\Users\dasj4\.m2\repository\org\hibernate\validator\hibernate-validator\6.0.18.Final\hibernate-validator-6.0.18.Final.jar  
**MD5:** d3eeb4f1bf013d939b86dfc34b0c6a5d  
**SHA1:** 7fd00bcd87e14b6ba66279282ef15efa30dd2492  
**SHA256:**79fb11445bc48e1ea6fb259e825d58b3c9a5fa2b7e3c9527e41e4aeda82de907  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final](https://ossindex.sonatype.org/component/pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aredhat&cpe_product=cpe%3A%2F%3Aredhat%3Ahibernate_validator&cpe_version=cpe%3A%2F%3Aredhat%3Ahibernate_validator%3A6.0.18)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

[**CVE-2020-10693**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693)  suppress

A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.

CWE-20 Improper Input Validation  
  
CVSSv2:

* Base Score: MEDIUM (5.0)
* Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSSv3:

* Base Score: MEDIUM (5.3)
* Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:

* - [[portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219](https://lists.apache.org/thread.html/rd418deda6f0ebe658c2015f43a14d03acb8b8c2c093c5bf6b880cd7c%40%3Cpluto-dev.portals.apache.org%3E)
* - [[portals-pluto-dev] 20210714 [jira] [Created] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219](https://lists.apache.org/thread.html/rf9c17c3efc4a376a96e9e2777eee6acf0bec28e2200e4b35da62de4a%40%3Cpluto-dev.portals.apache.org%3E)
* - [[portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-791 Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219](https://lists.apache.org/thread.html/rb8dca19a4e52b60dab0ab21e2ff9968d78f4b84e4033824db1dd24b4%40%3Cpluto-scm.portals.apache.org%3E)
* CONFIRM - <https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10693>
* MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
* OSSINDEX - [[CVE-2020-10693] CWE-20: Improper Input Validation](https://ossindex.sonatype.org/vulnerability/CVE-2020-10693?component-type=maven&component-name=org.hibernate.validator%2Fhibernate-validator&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions: ([show all](file:///C:\Users\dasj4\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html))

* [cpe:2.3:a:redhat:hibernate\_validator:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.0.0; versions up to (excluding) 6.0.20](https://web.nvd.nist.gov/view/vuln/search-results?adv_search=true&cves=on&cpe_version=cpe%3A%2Fa%3Aredhat%3Ahibernate_validator)
* ...

**jboss-logging-3.4.1.Final.jar**

**Description:**

The JBoss Logging Framework

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\jboss\logging\jboss-logging\3.4.1.Final\jboss-logging-3.4.1.Final.jar  
**MD5:** 52ee373b84e39570c78c0815006375bc  
**SHA1:** 40fd4d696c55793e996d1ff3c475833f836c2498  
**SHA256:**8efe877d93e5e1057a1388b2950503b88b0c28447364fde08adbec61e524eeb8  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.jboss.logging/jboss-logging@3.4.1.Final](https://ossindex.sonatype.org/component/pkg:maven/org.jboss.logging/jboss-logging@3.4.1.Final?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**classmate-1.5.1.jar**

**Description:**

Library for introspecting types with full generic information

including resolving of field and method types.

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\com\fasterxml\classmate\1.5.1\classmate-1.5.1.jar  
**MD5:** e91fcd30ba329fd1b0b6dc5321fd067c  
**SHA1:** 3fe0bed568c62df5e89f4f174c101eab25345b6c  
**SHA256:**aab4de3006808c09d25dd4ff4a3611cfb63c95463cfd99e73d2e1680d229a33b  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/com.fasterxml/classmate@1.5.1](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml/classmate@1.5.1?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)

**spring-web-5.2.3.RELEASE.jar**

**Description:**

Spring Web

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\spring-web\5.2.3.RELEASE\spring-web-5.2.3.RELEASE.jar  
**MD5:** a89d66690cd14159aa6ac1e875e54411  
**SHA1:** dd386a02e40b915ab400a3bf9f586d2dc4c0852c  
**SHA256:**25d264969c624cb8103a7f2b36b148ea1be8b87780c4758e7f9a6e2bc8416d76  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.springframework/spring-web@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-web@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

**CVE-2016-1000027** (OSSINDEX)  suppress

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

CWE-502 Deserialization of Untrusted Data  
  
CVSSv2:

* Base Score: HIGH (9.8)
* Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

References:

* OSSINDEX - [[CVE-2016-1000027] CWE-502: Deserialization of Untrusted Data](https://ossindex.sonatype.org/vulnerability/CVE-2016-1000027?component-type=maven&component-name=org.springframework%2Fspring-web&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

**spring-beans-5.2.3.RELEASE.jar**

**Description:**

Spring Beans

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\spring-beans\5.2.3.RELEASE\spring-beans-5.2.3.RELEASE.jar  
**MD5:** b64e8da412c3b6100f4bc0f54325d44f  
**SHA1:** 0250c8c641433dc06b1b44e4563fa08a2fbf8954  
**SHA256:**d3083070ad4eaf32e003b86ca0e7c0cb4fd2819800fef86ceb1043d387c14e2d  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

**CVE-2022-22965** (OSSINDEX)  suppress

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')  
  
CVSSv2:

* Base Score: HIGH (9.8)
* Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

References:

* OSSINDEX - [[CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')](https://ossindex.sonatype.org/vulnerability/CVE-2022-22965?component-type=maven&component-name=org.springframework%2Fspring-beans&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-beans:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

**spring-webmvc-5.2.3.RELEASE.jar**

**Description:**

Spring Web MVC

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\spring-webmvc\5.2.3.RELEASE\spring-webmvc-5.2.3.RELEASE.jar  
**MD5:** 867cc7369d453637b5042ee4d6931a78  
**SHA1:** 745a62502023d2496b565b7fe102bb1ee229d6b7  
**SHA256:**b3b0a2477e67b050dd5c08dc96e76db5950cbccba075e782c24f73eda49a0160  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

**CVE-2021-22060** (OSSINDEX)  suppress

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

CWE-117 Improper Output Neutralization for Logs  
  
CVSSv2:

* Base Score: MEDIUM (4.3)
* Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

References:

* OSSINDEX - [[CVE-2021-22060] CWE-117: Improper Output Neutralization for Logs](https://ossindex.sonatype.org/vulnerability/CVE-2021-22060?component-type=maven&component-name=org.springframework%2Fspring-webmvc&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-webmvc:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

**spring-context-5.2.3.RELEASE.jar**

**Description:**

Spring Context

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\spring-context\5.2.3.RELEASE\spring-context-5.2.3.RELEASE.jar  
**MD5:** a5ba542a35f3c9fca630df1715ccf325  
**SHA1:** 7750c95c96c7a1885c8b1b503ba915bc33ca579a  
**SHA256:**82c625cffed80685b153700359a6c6d5c91018069a0171cf21a7defb0267e993  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.springframework/spring-context@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-context@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

**CVE-2022-22968** (OSSINDEX)  suppress

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity  
  
CVSSv2:

* Base Score: MEDIUM (5.3)
* Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

References:

* OSSINDEX - [[CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity](https://ossindex.sonatype.org/vulnerability/CVE-2022-22968?component-type=maven&component-name=org.springframework%2Fspring-context&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-context:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

**spring-expression-5.2.3.RELEASE.jar**

**Description:**

Spring Expression Language (SpEL)

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\spring-expression\5.2.3.RELEASE\spring-expression-5.2.3.RELEASE.jar  
**MD5:** f2d2fe0e4f9b9b23b03d07839393de5a  
**SHA1:** d0c6bb10758805b2153c589686b8045554bfac2d  
**SHA256:**1ba798e1f4da9e5ad68e67d7e7abe39f141674762c8755d952edeb0380d384b9  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Identifiers**

* [pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress

**Published Vulnerabilities**

**CVE-2022-22950** (OSSINDEX)  suppress

n Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling  
  
CVSSv2:

* Base Score: MEDIUM (6.5)
* Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:

* OSSINDEX - [[CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling](https://ossindex.sonatype.org/vulnerability/CVE-2022-22950?component-type=maven&component-name=org.springframework%2Fspring-expression&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-expression:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

**CVE-2023-20861** (OSSINDEX)  suppress

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-noinfo  
  
CVSSv2:

* Base Score: MEDIUM (6.5)
* Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:

* OSSINDEX - [[CVE-2023-20861] CWE-noinfo](https://ossindex.sonatype.org/vulnerability/CVE-2023-20861?component-type=maven&component-name=org.springframework%2Fspring-expression&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-expression:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

**CVE-2023-20863** (OSSINDEX)  suppress

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')  
  
CVSSv2:

* Base Score: MEDIUM (6.5)
* Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:

* OSSINDEX - [[CVE-2023-20863] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')](https://ossindex.sonatype.org/vulnerability/CVE-2023-20863?component-type=maven&component-name=org.springframework%2Fspring-expression&utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)

Vulnerable Software & Versions (OSSINDEX):

* cpe:2.3:a:org.springframework:spring-expression:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*

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

**Description:**

Spring Core

**License:**

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

**File Path:** C:\Users\dasj4\.m2\repository\org\springframework\spring-core\5.2.3.RELEASE\spring-core-5.2.3.RELEASE.jar  
**MD5:** ae11e44d9eff630186b9e095e70b59de  
**SHA1:** 3734223040040e8c3fecd5faa3ae8a1ed6da146b  
**SHA256:**6df908f4deaeefd2b03b56a00246cc0dc0d941d9636e811025bc6fc5a2a44851  
**Referenced In Project/Scope:**rest-service:compile

**Evidence**

**Related Dependencies**

**Identifiers**

* [pkg:maven/org.springframework/spring-core@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-core@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0)  (*Confidence*:High)
* [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress
* [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  (*Confidence*:Highest)  suppress

**5. Mitigation Plan**

Interpret the results from the manual review and static testing report. Then identify the steps to mitigate the identified security vulnerabilities for Artemis Financial’s software application.

For my mitigation plan it’s important to address the vulnerabilities found in the review and testing is essential to ensure their security. Firstly, to prevent SQL injection attacks as the company should use secure coding practices like parameterized queries, which treat user inputs as data rather than executable commands. For encrypting sensitive information stored in databases with strong encryption will protect data from unauthorized access. Using secure key management practices will further enhance this protection. To avoid XSS attacks, it's important to sanitize user inputs and encode outputs to prevent harmful scripts from being injected. API endpoints should be secured with strong authentication methods and protected with rate limiting to prevent abuse. Regularly updating open-source libraries and components will also help address vulnerabilities from outdated software. Lastly, to handle errors securely by configuring messages so they don’t reveal sensitive information about the system. Using generic error messages will help protect the system from potential attacks. With these steps in mind Artemis Financial can improve its security, protect against potential threats, and ensure it meets regulatory requirements.