****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Artemis Financial Vulnerability Assessment Report 1](#_Toc117445625)

[Document Revision History 3](#_Toc117445626)

[Client 3](#_Toc117445627)

[Developer 3](#_Toc117445628)

[1. Interpreting Client Needs 3](#_Toc117445629)

[2. Static Testing 4](#_Toc117445630)

[3. Manual Review 5](#_Toc117445631)

[1. Mitigation Plan 15](#_Toc117445632)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **09.22.2022** | **Marcus J. Wilson** |  |

## Client



## Developer

Marcus J. Wilson

## Interpreting Client Needs

Review the scenario to determine your client’s needs and potential threats and attacks associated with their application and software security requirements.Document your findings in your vulnerability assessment report. Consider the scenario information and the following questions regarding how companies protect against external threats:

* 1. What is the value of secure communications to the company?
     1. The value of secure communications to Artemis financial is imperative as the firm develops individualized financial plans for their clients, which include savings, retirement, investments, and insurance. The individualized plans include a lot of sensitive data, which the company would not want to be transferred through an unsecure process, and potentially end up in the wrong hands.
  2. Does the company make any international transactions?
     1. Artemis Financial doesn’t appear to make international transactions; however, the company states they’re looking into modernizing their operations, perhaps this could include expanding their offerings to conduct international business.
  3. What external threats might be present now and in the immediate future?
     1. An external threat that is present now and will continue to be present for the foreseeable future, is SQL injection. SQL Injection can be devastating to a company, or even an individual, as untrusted data is exactly as it sounds, information that cannot be trusted; thus, potentially leading to stolen sensitive information, or gain elevated privileges.
  4. What are the modernization requirements that you must consider? For example:
     1. The role of open-source libraries
        1. The role of open-source libraries brings forth an era of transparency, allowing anyone to view company ‘secrets’, which also plays a role in the creation of morally and ethically accurate algorithms.
     2. Evolving web application technologies.

## Static Testing

* 1. The names or vulnerability codes of the known vulnerabilities

Graphical user interface, text, application

Description automatically generated

## 

## Manual Review

|  |  |  |
| --- | --- | --- |
| **Dependency** | **CPE** | **Summary** |
| log4j-api-2.12.1.jar | [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) | The Apache Log4j API |
| tomcat-embed-core-9.0.30.jar | [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) | Core Tomcat implementation |
| spring-core-5.2.3.RELEASE.jar | [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) | Spring Core |
| spring-boot-2.2.4.RELEASE.jar | [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) [cpe:2.3:a:vmware:spring\_framework: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_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A2.2.4) | Spring Boot |
| spring-boot-starter-validation-2.2.4.RELEASE.jar | [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) | Starter for using Java Bean Validation with Hibernate Validator |
| snakeyaml-1.25.jar | [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) | YAML 1.1 parser and emitter for Java |
| jackson-databind-2.10.2.jar | [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Afasterxml&cpe_product=cpe%3A%2F%3Afasterxml%3Ajackson-databind&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson-databind%3A2.10.2) | General data-binding functionality for Jackson: works on core streaming API |
| bcprov-jdk15on-1.46.jar | [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) | 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. |
| logback-core-1.2.3.jar | [cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aqos&cpe_product=cpe%3A%2F%3Aqos%3Alogback&cpe_version=cpe%3A%2F%3Aqos%3Alogback%3A1.2.3) | logback-core module |
| hibernate-validator-6.0.18.Final.jar | [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) | Hibernate's Bean Validation (JSR-380) reference implementation. |

|  |  |  |
| --- | --- | --- |
| **CPE**  **Vulnerability ID | Severity CVSS: v3.1 | v2.0**  **CVE Summary** | **Mitigation** | |
| [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)  **1. CVE-2021-44832 | 6.6 | 8.5**  Versions of Apache Log4j2 are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server.  **2. CVE-2021-45105 | 5.9 | 4.3**  Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups.  **3. CVE-2021-45046 | 9.0 | 5.1**  It was found that the fix to address CVE-2021-44228 in  Apache Log4j 2.15.0 was incomplete in certain non-default  Configurations  **4. CVE-2021-44228 | 10.0 | 9.3**  Apache Log4j2 2.0-beta9 through 2.15.0, JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints.  **5. CVE-2020-9488 | 3.7 | 4.3**  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. | 1. This issue is fixed by limiting JNDI data source names to the java protocol in  Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.  2. Fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.  3. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.  4. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed.  5. Fixed in Apache Log4j 2.12.3 and 2.13.1 | |
| [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)  **1. CVE-2019-17569 | 4.8 | 5.8**  The refactoring introduced a regression.    **2. CVE-2019-17569 | 4.8 | 5.8**  A specially crafted sequence of HTTP/2 requests could trigger high CPU usage for several seconds.  **3. CVE-2019-17569 | 4.8 | 5.8**  An h2c direct did not release the HTTP/1.1 processor after the upgrade to HTTP/2.  **4. CVE-2019-17569 | 4.8 | 5.8**  The payload length in a WebSocket frame was not correctly. Invalid payload lengths could trigger an infinite loop.  **5. CVE-2019-17569 | 4.8 | 5.8**  If an HTTP/2 client exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers.  **6. CVE-2019-17569 | 4.8 | 5.8**  While investigating bug 64830 it was discovered that certain versions of Apache Tomcat, could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream.  **7. CVE-2019-17569 | 4.8 | 5.8**  Certain versions of Apache Tomcat, the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid.  **8. CVE-2019-17569 | 4.8 | 5.8**  Certain versions of Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required.  **9. CVE-2019-17569 | 4.8 | 5.8**  An Incorrect Default Permissions vulnerability in the packaging of certain Tomcat versions, allows local attackers to escalate from group tomcat to root.  **10. CVE-2019-17569 | 4.8 | 5.8**  Certain versions of Tomcat:   1. An attacker can control the contents and name of a file on the server 2. The server is configured to use the PersistenceManager with a FileStore 3. The PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized 4. The attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control.   **11. CVE-2019-17569 | 4.8 | 5.8**  When serving resources from a network location using the NTFS file system, certain versions of Apache Tomcat were susceptible to JSP source code disclosure in some configurations.  **12. CVE-2019-17569 | 4.8 | 5.8**  When using certain versions of Apache Tomcat with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494.  **13. CVE-2019-17569 | 4.8 | 5.8**  A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm.  **14. CVE-2019-17569 | 4.8 | 5.8**  Certain versions of Apache did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy.  **15. CVE-2019-17569 | 4.8 | 5.8**  Certain versions of Apache Tomcat did not properly validate incoming TLS packets.  **16. CVE-2019-17569 | 4.8 | 5.8**  The documentation within certain Apache Tomcat versions, EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network.  **17. CVE-2019-17569 | 4.8 | 5.8**  In certain Apache Tomcat versions the Form authentication example in the example’s web application displayed user provided data without filtering, exposing a XSS vulnerability. | 1. Update to Apache Tomcat 9.0.40 or later  2. Update to Apache Tomcat 9.0.40 or later  3. Update to Apache Tomcat 9.0.40 or later  4. Update to Apache Tomcat 9.0.40 or later  5. Update to Apache Tomcat 9.0.40 or later  6. Update to Apache Tomcat 9.0.40 or later  7. Update to Apache Tomcat 9.0.40 or later  8. Update to Apache Tomcat 9.0.40 or later  9. An update that fixes one vulnerability issue is now available. To install openSUSE Security Update use the SUSE recommended installation methods, such as YaST online update or “zypper patch”  10. Update to Apache Tomcat 9.0.40 or later  11. Update to Apache Tomcat 9.0.40 or later  12. N/A  13. Update to Apache Tomcat 9.0.40 or later  14. Update to Apache Tomcat 9.0.40 or later  15. Update to Apache Tomcat 9.0.40 or later  16. Users running clustering over an untrusted network who require full protection should switch to an alternative solution such as running the clustering communication over a VPN.  17. Update to Apache Tomcat 9.0.40 or later | |
| [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3)  **1. CVE-2022-22971 | 3.1 | 2.0**  In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.  **2. CVE-2022-22970 | 5.3 | 3.5**  In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.   1. **CVE-2022-22968 | 5.3 | 5.0**   In Spring Framework the patterns for dissallowedFields 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.   1. **CVE-2022-22965 | 9.8 | 7.5**   A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.   1. **CVE-2022-22950 | 4.3 | 4.0**   Certain Spring Framework versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.   1. **CVE-2022-22060 | 4.3 | 4.0**   Certain Spring Framework versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.   1. **CVE-2022-22096 | 7.8 | 4.6**   Certain Spring Framework versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.   1. **CVE-2022-22118 | 7.8 | 4.6**   Certain Spring Framework versions, a WebFlux application is vulnerable to a privilege escalation.   1. **CVE-2022-5421 | 6.5 | 3.6**   Certain Spring Framework versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.   1. **CVE-2022-1000027 | 9.8 | 7.5**   Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. | * + 1. Users should upgrade to 5.3.20     2. Users should upgrade to 5.3.20     3. Users should upgrade to 5.3.19+     4. Users should upgrade to 5.3.19+     5. Users should upgrade to 5.3.19+     6. Users should upgrade to 5.3.19+     7. Users should upgrade to 5.3.19+     8. Users should upgrade to 5.3.7+     9. Users should upgrade to 5.3.7+     10. Users should upgrade to 5.3.7+ |
| [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)   * + - 1. CVE-2022-27772 | 7.8 | 4.6   spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking | * + - * 1. This vulnerability is patched in versions v2.2.11.RELEASE or later |
| [cpe:2.3:a:vmware:spring\_framework: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_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A2.2.4)  **CVE-2022-22970 | 5.3 | 3.5**  In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.   * + - 1. **CVE-2022-22968 | 5.3 | 5.0**   In Spring Framework the patterns for dissallowedFields 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.   * + - 1. **CVE-2022-22965 | 9.8 | 7.5**   A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.   * + - 1. **CVE-2022-22950 | 4.3 | 4.0**   Certain Spring Framework versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.   * + - 1. **CVE-2020-5421 | 6.5 | 3.6**   In certain versions of Spring, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.   * + - 1. **CVE-2016-1000027 | 9.8 | 7.5**   Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data.   * + - 1. **CVE-2018-11040 | 7.5 | 4.3**   Certain versions of Spring Framework, allows web applications to enable cross-domain requests via JSONP (JSON with Padding) through AbstractJsonpResponseBodyAdvice for REST controllers and MappingJackson2JsonView for browser requests.   * + - 1. **CVE-2018-11039 | 5.9 | 4.3**   Certain versions of Spring Framework, allow web applications to change the HTTP request method to any HTTP method (including TRACE) using the HiddenHttpMethodFilter in Spring MVC  9. **CVE-2018-1257 | 6.5 | 4.0**  Certain versions of Spring Framework, allows applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module.  10. **CVE-2018-1270 | 9.8 | 7.5**  Certain versions of Spring Framework, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module.   * + 1. **CVE-2014-0054 | N/A | 6.8**   The Jaxb2RootElementHttpMessageConverter in Spring MVC in Spring Framework before 3.2.8 and 4.0.0 before 4.0.2 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue.   * + 1. **CVE-2013-7315 | N/A | 6.8**   The Spring MVC in Spring Framework before 3.2.4 and 4.0.0.M1 through 4.0.0.M2 does not disable external entity resolution for the StAX XMLInputFactory. This allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML with JAXB, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152.   * + 1. **CVE-2013-4152 | N/A | 6.8**   The Spring OXM wrapper in Spring Framework before 3.2.4 and 4.0.0.M1, when using the JAXB marshaller, does not disable entity resolution. | Users should upgrade to 5.3.20  Users should upgrade to 5.3.19+  Users should upgrade to 5.3.19+  Users should upgrade to 5.3.19+  Users should be upgraded to 5.1.18 at least.  This was fixed upstream by detailing HttpInvoker endpoints should not be exposed to untrusted clients, these upstream changes would of been included with Fuse 6.3 R5; which included a version change to 3.2.18  5.0.x users should upgrade to 5.0.7; 4.3.x users should upgrade to 4.3.18  5.0.x users should upgrade to 5.0.7; 4.3.x users should upgrade to 4.3.18  5.0.x users should upgrade to 5.0.7; 4.3.x users should upgrade to 4.3.18  5.0.x users should upgrade to 5.0.7; 4.3.x users should upgrade to 4.3.18  Red Hat JBoss Fuse 6.1.0, which fixes multiple security issues, several bugs, and adds various enhancements, is now available from the Red Hat Customer Portal  Users of 3.x should upgrade to 3.2.4 or later; Users of 4.x should upgrade to 4.0.0.RC1 or later.  Red Hat JBoss SOA Platform 5.3.1 roll up patch 4, which fixes two security issues and various bugs, is now available from the Red Hat Customer Portal. |
| [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)   1. **CVE-2022-38751 | 6.5 | N/A**   Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS).  **2. CVE-2022-38750 | 5.5 | N/A**  Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS).   1. **CVE-2022-38749 | 6.5 | N/A**   Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS).   1. **CVE-2022-25857 | 7.5 | N/A**   The package org.yaml:snakeyaml from 0 and before 1.31 are vulnerable to Denial of Service (DoS) due missing to nested depth limitation for collections.   1. **CVE-2017-18640 | 7..5 | 5.0**   The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564. | 1. Update delivered in version 1.31 2. Update delivered in version 1.31 3. Update delivered in version 1.31 4. Update delivered in version 1.31 5. Update delivered in version 1.31 |
| [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Afasterxml&cpe_product=cpe%3A%2F%3Afasterxml%3Ajackson-databind&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson-databind%3A2.10.2)   1. **CVE-2020-36518 | 7.5 | 5.0**   jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.  2. **CVE-2020-25649 | 7.5 | 5.0**  A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly | 1. We recommend that you upgrade your jackson-databind packages, 2. Fixed in 2.11.0, and as a consequence also fixed in 2.12.0. |
| [cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aqos&cpe_product=cpe%3A%2F%3Aqos%3Alogback&cpe_version=cpe%3A%2F%3Aqos%3Alogback%3A1.2.3)   1. CVE-2021-42550 | 6.6 | 8.5   In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers. | 1. Update to Logback 1.3.x |
| [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)   1. CVE-2021-42550 | 6.6 | 8.5   In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers. | 1. Update to version 1.2.9 |
| [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)  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. | Fixed in version 6.0.20 + |
| [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)   1. CVE-2016-1000352 | 7.4 | 5.8   In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode   1. CVE-2016-1000346 |3.7 | 4.3   In the Bouncy Castle JCE Provider version 1.55 and earlier the other party DH public key is not fully validated. This can cause issues as invalid keys can be used to reveal details about the other party's private key where static Diffie-Hellman is in use   1. CVE-2016-1000345 | 5.9 | 4.3   In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES/ECIES CBC mode vulnerable to padding oracle attack.   1. CVE-2016-1000344 |7.4 | 5.8   In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES implementation allowed the use of ECB mode.   1. CVE-2016-1000343 | 7.5 | 5.0   In the Bouncy Castle JCE Provider version 1.55 and earlier the DSA key pair generator generates a weak private key if used with default values.   1. CVE-2016-1000342 |7.5 | 5.0   In the Bouncy Castle JCE Provider version 1.55 and earlier ECDSA does not fully validate ASN.1 encoding of signature on verification.   1. CVE-2016-1000341 | 5.9 | 4.3   In the Bouncy Castle JCE Provider version 1.55 and earlier DSA signature generation is vulnerable to timing attack.   1. CVE-2016-1000339 | 5.3 | 5.0   In the Bouncy Castle JCE Provider version 1.55 and earlier the primary engine class used for AES was AESFastEngine.   1. CVE-2016-1000338 | 7.5 | 5.0   In Bouncy Castle JCE Provider version 1.55 and earlier the DSA does not fully validate ASN.1 encoding of signature on verification.   1. CVE-2018-5382 | 4.4 | 3.6   The default BKS keystore use an HMAC that is only 16 bits long, which can allow an attacker to compromise the integrity of a BKS keystore.   1. CVE-2017-13098 | 5.9 | 4.3   BouncyCastle TLS prior to version 1.0.3, when configured to use the JCE (Java Cryptography Extension) for cryptographic functions, provides a weak Bleichenbacher oracle when any TLS cipher suite using RSA key exchange is negotiated.   1. CVE-2013-1624 | N/A | 4.0   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. | 1. This mode is regarded as unsafe and support for it has been removed from the provider. 2. As of release 1.56 the key parameters are checked on agreement calculation. 3. Users should update to versions of Bouncy Castle JCE Provide > v1.55. 4. This mode is regarded as unsafe and support for it has been removed from the provider. 5. In earlier releases this can be dealt with by explicitly passing parameters to the key pair generator. Otherwise, update to versions of Bouncy Castle JCE Provide > v1.55. 6. Users should update to versions of Bouncy Castle JCE Provide > v1.55. 7. Users should update to versions of Bouncy Castle JCE Provide > v1.55. 8. Users should update to versions of Bouncy Castle JCE Provide > v1.55. 9. Users should update to versions of Bouncy Castle JCE Provide > v1.55. 10. Bouncy Castle release 1.47 changes the BKS format to a format which uses a 160 bit HMAC instead. This applies to any BKS keystore generated prior to BC 1.47. For situations where people need to create the files for legacy reasons a specific keystore type "BKS-V1" was introduced in 1.49. 11. Users should update to versions of Bouncy Castle JCE Provide > v1.55. 12. Users should update to versions of Bouncy Castle JCE Provide > v1.55. |

## Mitigation Plan

I believe a good reason for filtering false positives is so you do not over clutter your dependency report with unnecessary text, such as the multiple instances of the same CPE, or Vulnerable ID.