****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Document Revision History 3](#_Toc32574607)

[Client 3](#_Toc32574608)

[Instructions 3](#_Toc32574609)

[Developer 4](#_Toc32574610)

[1. Interpreting Client Needs 4](#_Toc32574611)

[2. Areas of Security 4](#_Toc32574612)

[3. Manual Review 4](#_Toc32574613)

[4. Static Testing 4](#_Toc32574614)

[5. Mitigation Plan 4](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **14 September 2023** | **Andre Burton** | **Initial Report** |

## Client



## Developer

Andre Burton

## Interpreting Client Needs

My client Artemis Financial is a company that consults its customers with financial plans that include savings, retirement, investment, and insurance accounts. This client is looking to modernize their operations and wants the best software security available. This company puts high value on secure communications and uses a RESTful web API. Due to the client’s information shared with their customers it’s imperative to secure all information regarding finances between the client and their customers. The client didn’t say whether they deal with international transactions, but the security should be developed so will be protected from any threats anywhere in the world. There will be government restrictions on secure communications which the client should keep in mind, these restrictions could include following current privacy acts laid out by the government. They will also have to follow the current rules and laws regarding secure communications and must expand that to all counties that they have customers in. There are many types of threats that can be present currently and in the immediate future these include threats to the clients and their customers. Client threats can include malicious bugs, exploits, hacking, etc. These can include a combination of cross-site scripting, cross-site request forgery, man-in-the-middle, session hijacking/fixation, and a few others that play a role in web-based programming which can be threats to the client. On the customer side they could see threats such as click-jacking, hacking, phishing, and other types of common attacks targeted towards the customer but may affect the client as well. These threats are real and can affect both the client and tis customer both now and in the future, with the proper security put into place and security upkeep will prevent many of these issues from happening. To modernize the systems, we need to update all the systems to the newest system types, implement two-factor authentication for the client’s customers, proper input validations software, and to have proper client/server connection security put in place. Adding new levels of security will help but we must first check for updates to the current systems and ensure proper maintenance is completed on them to ensure no security threats happen.

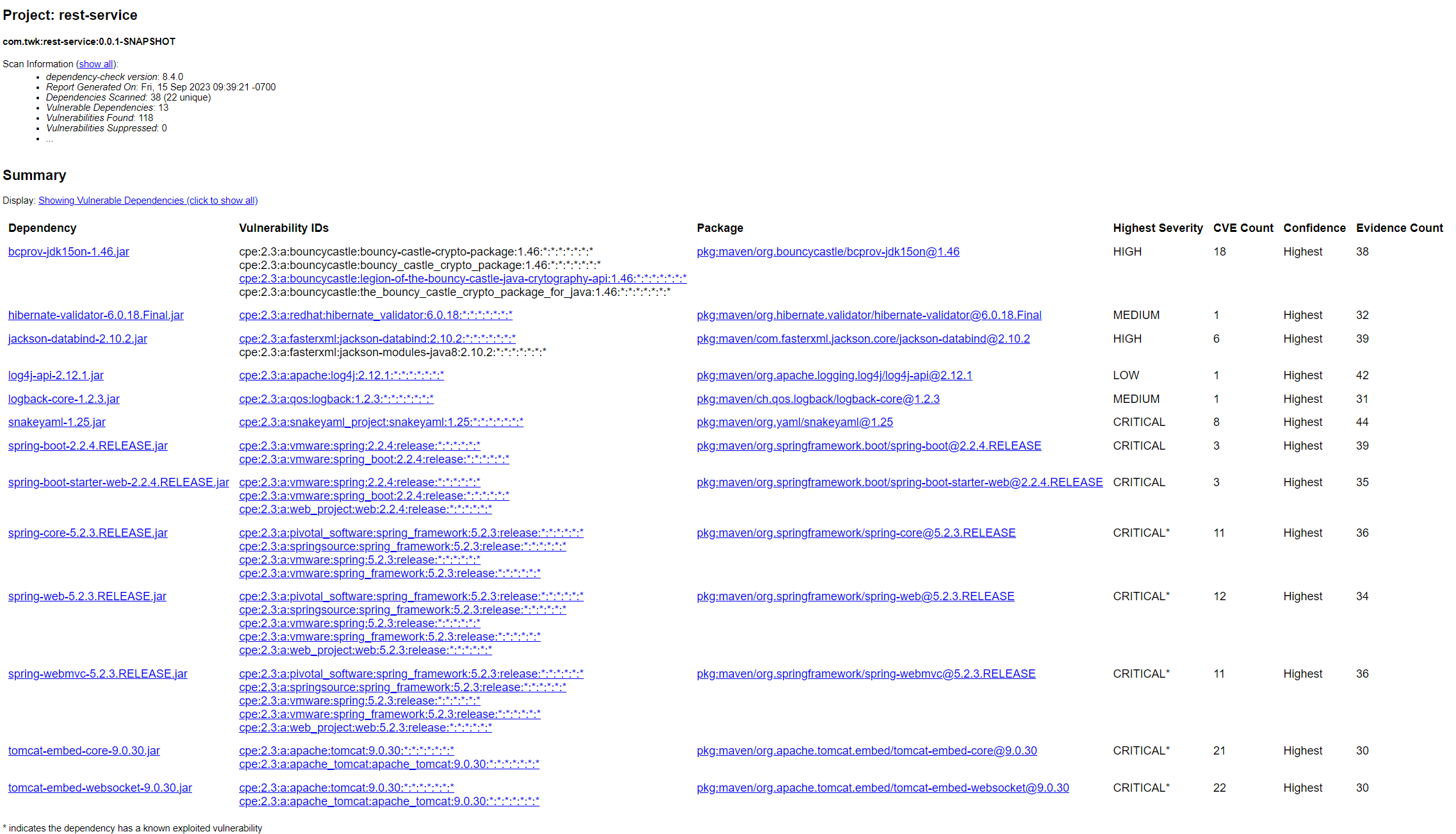
## Areas of Security

After reviewing the client’s needs and comparing them to the vulnerability assessment process flow diagram the areas of security that apply to my clients’ needs are **input validation, secure API’s, cryptography, code error, and encapsulation**. Input validation was picked due to verifying user inputs which will prevent unauthorized inputs. Secure API was chosen because the system runs off an API and due to the client working with finical information it protects transaction information between transfers. Cryptography was chosen due to it encrypting sensitive data which blocks that information from attackers. Code error was chosen for when errors occur it keeps track of it and reports it while at the same time gives the users a generic message which prevents attacks from knowing what is going on. And lastly encapsulation was picked due to the large amount of sensitive data the client possesses and this helped to ensure only authorized people are granted access to different levels of information. Client/server and code quality were not chosen because client/server due to the client not needing secure distributed computing services and code quality wasn’t chosen because the company is already using RESTful web API and won’t need it up to this point, but its important to know as the company grows the areas of security will change as well.

## Manual Review

After manually reviewing the code base I can see a few initial issues that would need to be fixed. To start there doesn’t seem to be any presence of authentication which will need to be added due to the information that the client is using. The second seen issue was the use of HHTP vs HHTPS which also helps with the encryption of readable data when transferred between the server and the client. The next seen issue with the base code is no seen authentication which means there’s no way to ensure and confirm the user’s identity. The next issue is there seems to be no validation which verifies the software’s purpose. These are some of more serious issues that would need to be fixed in order to secure the software properly.

## Static Testing



|  |  |  |
| --- | --- | --- |
| Name/Vulnerability Code | Brief Description | Attribution |
| [bcprov-jdk15on-1.46.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | This is called a “bouncy castle crypto package” and is a java implementation of cryptographic algorithms and falls into the high severity range. This dependency had 18 different vulnerabilities with most targeting version 1.55 and earlier. A solution for this would be to update it to the most current version. | This issue was found due to the DSA key pair generator generating a weak private key if it was sued with default values. They also found some of the vulnerabilities allowed use of ECB mode and was unsafe. They also found it was vulnerable to timing attacks which allows attackers access to signature K values and private values as well. They also found other numerous exploits and issues which lead to support being removed |
| [hibernate-validator-6.0.18.Final.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l3_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | This is called a “hibernate Bean Validation” and is a reference implementation and affected versions from 5.0.0 up to version 6.0.20. This dependency falls into the medium severity category. A solution for this fix would be to update to the current version. | This flaw was found in the version 6.1.2 final and allowed invalid EL expression to be evaluated as if they were valid which allowed attackers to bypass input controls that were put in place to handle data in error messages. |
| [jackson-databind-2.10.2.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | This is called “General data-binding functionality for Jackson” and works with the core streaming API. This falls into the high severity category and has 6 different vulnerabilities. The fix for this issue was updating to the most current version or disable external entity expansion. | This flaw was found in fasterXMl and did not have entity expansion secured properly which allows vulnerability to XML external entity attacks and greatly affected data integrity. This had numerous versions of issues all the way up to version 2.15.2 |
| [log4j-api-2.12.1.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l10_a55e6d987f50a515c9260b0451b4fa217dc539cb) | This falls into the low severity category. This had improper validation of certificates with host mismatch in SMTP appended which allows SMTPS connection to be intercepted by man-in-the-middle attacks. The fix for this was to update to 2.12.3 or 2.13.1 | No information regarding how this vulnerability had been identified or documented in the past. |
| [logback-core-1.2.3.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l12_864344400c3d4d92dfeb0a305dc87d953677c03c) | Also known as the “log-core module”. This falls into the medium severity category. This affected version 1.2.7 and earlier and allows attackers edit configuration files and could implement malicious configurations and execute arbitrary code to load from the LDAP servers. The fix for this was to update to the current version or using certificate pinning. | No information regarding how this vulnerability had been identified or documented in the past. |
| [snakeyaml-1.25.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | Also known as “YAML 1.1 parser and emitter” and falls into the critical severity category”. This affected versions up to 1.31 and had 8 vulnerabilities built into it. The fix for this was to update to the most current version or using SnakeYaml’s SafeContrurctor. This was caused by vulnerabilities to denial of service due to missing to nested depth limitation for collections which allowed attackers to supply content that would cause the parser to crash by stack overflow. | No information regarding how this vulnerability had been identified or documented in the past. |
| [spring-boot-2.2.4.RELEASE.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l15_225a4fd31156c254e3bb92adb42ee8c6de812714) | This falls into the critical category with 3 different vulnerabilities and affects versions 3.0.0-3.0.5 and 2.7.0-2.7.10 and older versions. The issue was applications deployed to cloud foundry could be susceptible to security bypass. The fix for this would be 3.0 users should upgrade to versions 3.0.6 and 2.7 users should upgrade to 2.7.11. These older versions resulted in temporary directory hijacking. In other versions there was also potential for denial-of-service attacks if the spring MVC was used together with a reverse proxy cache | No information regarding how this vulnerability had been identified or documented in the past. |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l16_ec75d01d212b5229c16d872fb127744c0ed46ed8) | This falls into the critical severity category and has 3 different vulnerabilities. This affected versions 3.0.0-3.0.5 and 2.7.0-2.7.10 and other unsupported versions. This was caused by an application deployed to cloud foundry that could be susceptible to security bypass. There was also potential for denial-of-service attacks if the spring MVC was used together with a reverse proxy cache. The fix for this issue was to update to the most current version. | No information regarding how this vulnerability had been identified or documented in the past. |
| [spring-core-5.2.3.RELEASE.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l17_3734223040040e8c3fecd5faa3ae8a1ed6da146b) | This falls into the critical severity category and has 11 vulnerabilities. This affected many versions and had numerous issues that caused multiple points of exploits. When using older versions locally authenticated malicious users could read/modify files, cause denial of service conditions, create vulnerability to a denial-of-service attack, and users can provide malicious input to cause the insertion of additional log entries. The fix for this issue is to update to the latest version. | No information regarding how this vulnerability had been identified or documented in the past. |
| [spring-web-5.2.3.RELEASE.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l18_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | This falls into the critical category and has 12 vulnerabilities. These were cause by remote code execution vulnerabilities caused by data binding, privilege escalation caused by creating temporary storage directory’s, specially crafted expressions that may cause denial of service conditions, denial of service attacks caused by vulnerabilities in a stomp over websocket endpoints, and a few other exploits that cause issues. The fix for many of these was to update the most current system for a few resolutions may be if the application is deployed as a spring boot executable jar. | No information regarding how this vulnerability had been identified or documented in the past. |
| [spring-webmvc-5.2.3.RELEASE.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l19_745a62502023d2496b565b7fe102bb1ee229d6b7) | This falls into the critical severity category. This dependency has 11 different vulnerabilities which affect it. The majority of these are affected by vulnerabilities to remote code execution via data binding. This can be fixed with updates to the current version or if the application is deployed as a spring boot executable jar. Another fix would be the user of a jsessionis path parameter. Different vulnerabilities have different fixes but for an update must fix the issues but if an update is possible using the other methods may work as a temporary fix. | No information regarding how this vulnerability had been identified or documented in the past. |
| [tomcat-embed-core-9.0.30.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l20_ad32909314fe2ba02cec036434c0addd19bcc580) | Also known as core tomcat implementation. This falls into the critical category and has 21 different vulnerabilities. These are caused by attackers exploiting connection trusts, requests triggering high CPU usage which could result in server unresponsiveness, out of memory exception thrown which result in denial of service, multiple invalid requests could result in denial of service, connection issues resulting in information leaking between request, DoS risks, and multiple others. The fix for this is primary updating to the most current versions, and configuration changes. | No information regarding how this vulnerability had been identified or documented in the past. |
| [tomcat-embed-websocket-9.0.30.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l22_33157f6bc5bfd03380ebb5ac476db0600a04168d) | This is also known as core tomcat implementation. This falls into the critical category with 22 different vulnerabilities. These were caused by a combination of issues these being shared with the “[tomcat-embed-core-9.0.30.jar](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=91f5af1e2e&attid=0.1&permmsgid=msg-a:r-3439557073258669078&th=18a99baf617b8a5a&view=att&disp=inline&realattid=f_lmktxyw50&ser=1&saddbat=ANGjdJ9X00o8uFmQbu6HNQJcSYA0Sl7LudwNnXZi-WdSL2BeEHZ08LshJyNfaPaqVYyM8WMTVuwYGJSbtDBvEGwoB9UWxxBhkSzjnLkb0K8elia5NB7p_A6Lnvv0ZgTFY-bWCf0x-sN0ZO9lhD6rEavyJxKYTkUB20Yj6rQVGSf3o8S7IYdPtyrajq6jnyqRf3A9j4AcLIjEENc63xWVR9Yj30TtflwiDszg-GL-a61duIFn5YOHCQfL7g5QteHvdowqMNBKvca984HCgFzfQtEfq4tcsEeZFlLDQbyiNxFlcPvYS8nHQDUsMuCe9zciVAZjtLQrYrJrKsg8KMYXwVyQJCwpUg1Eh2Uh85chKdHGhSodPfsjlwn8J5LmG9yJUhP960C5NQoRGl76VMWUq0G2rPrsEbgy_F9pbnQZantOoerFjs-Y4O0-wBT4oxVZnn_6wvTE0ANiLJHFme7Zn2HkpDN8b3IcyId9GV0xjlCgHhbHfv1zjm_jekdL144H1u77tUsBFos0_2UY92NQ4b0vevXvNa_ovTykHRuUITh-2ImUJIKlOLfOTeoOuGJlhwR60OB5XXpE7TbYbLOp3E0Qmlb9EmRfwydOosZBDjg6vNClCIe4BtoP_MjJYMo9TIYCd5Vfjpm1lYbShn2AiyxSi8uqSBs73ep2aEIyOKorFnUYAVcF4mAci_a_DnCPWStNtRXosZfd7Hw4wg4tq3hvHLcovDauQ_8NxfzfuOUljRsUHnKJvpp0Mnc75ipYibOF15tyWYhLs2t2GrmkN-JuhIEgPUP5AhoRtEuXbw7xT5s0s3hYx2gpjwwx-LeHr-3EesNP4gAweySvljbLeQ1Pm-T7HlmcfW8ESeKGGJVmIKM52qg5SpQkL1x3LzG1zO2sg4cljjFXnR8r8dJY2npX-kK--qv7UoEO94W2bGCqdnsJvUlGc0S6gYbmTSIllmbW3y2pcjnFR046AfVGXFESJsU3Y6QG06wjE_uUtRSSIEcdTWJYScwc6yMtYauKjjBLBh7F7HJrMNPE3kpW#m__l20_ad32909314fe2ba02cec036434c0addd19bcc580)”. The fix for these were similar as well with fixes such as updating to the most current versions, and configuration changes. | No information regarding how this vulnerability had been identified or documented in the past. |

## 

## Mitigation Plan

After reviewing the results from the manual review and static testing report there are a few mitigation steps needed to put into place to fix the issues and prevent further issues. The first and easiest step would be to update all the dependencies to the most current version, this would correct a good portion of the issues. The second step would be to set configuration to the above dependency that that configuration issues. Third, we had some issues with XML parsers so configuring those so we could disable the external entity expansion. Next, we would need to verify certificate pinning in the vulnerabilities that had issues validating certificates. In conclusion, to mitigate the current issues we need to verify all of the above vulnerabilities are updated to the most current version, change setting configurations to prevent issues, and verify certificate issues and fix them accordingly.

Citations:

*National Institute of Standards and Technology*. NIST. (2023, September 13). https://www.nist.gov/