# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **03/30/2025** | **Skylr McKay** | **Completed entire document.** |

## 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

Skylr McKay

# 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?

Artemis investments as an organization is one that needs the most up to date and secure platforms of their RESTful web application as it is necessity to secure their customer bases financial plans that would include but not be limited to savings portfolios, retirement portfolios, investment portfolios, and insurance details meaning the optimization and streamlining of their web applications will ensure the ease and security of their clienteles personal information. With this in mind we first interpret the needs of the clients: to start Artemis Financial needs to have secure communications with their clients and while that is easily approachable it is crucial to the success of Artemis Financial due to the sensitive nature of their stored financial data and potential lawsuits and legal regulations that must be met to ensure business. That is where it is mandatory to ensure secure communication networking that protects against data leaks, breaches, and corruption while protecting against financial fraud and white collar crime all while maintaining the client trust. To lead we need to address that while Artemis Financial may not be a proprietor at this stage when it comes to international investments and transactions their update will potentially expand their reach meaning that the communication must comply with international security procedures and protections against cross-boarder crime and maintain cross-boarder cyber security. Leading further they must follow within their scopes governmental restrictions and guidelines which mandate the proper handling and securing of financial data. Finally Artemis Financial must be able to protect from external and internal threats that would compromise their client’s information like phishing, ransomware, inside jobs or man-in-the-middle, and many more that could compromise or bypass security. Afterwards it is with this that we must ensure regular modernization that would be prevalent like Open-Source Libraries and Evolving Web Application Technology needing regular updates for security.

# 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.

Authentication and Authorization: Authentication and Authorization is critical to the Client/Server connection as when paired with Logging and Monitoring is in place to ensure that encrypted data can only be accessed by authorized users and personnel. Considering the sensitivity of the data Artemis Financial has in their possession the requirement for verification procedures ensures that the data is not compromised by explorative attacks to the organization servers or potential leaking by lacking Authentication and Authorization.

Data Encryption: Data Encryption is another area of critical evaluation as the Sensitive data needs to be encrypted to ensure that if there is an attack on the server the locating and identification of sensitive data is delayed to ensure proper corrective action in a timely manner as it protects data in transit that could be intercepted and at rest during breaches caused by unauthorized access.

Input Validation: Input validation is another area of high evaluation as since users will be regularly using the web application it is imperative to ensure the prevention of injection attacks via validation and scrubbing of user inputs.

Error Handling: Error Handling is another element under study as it is imperative that error warnings don’t provide sensitive details of the system or the client as that could give hackers more resources to breach a server.

Session Management: Since this public resource that would be utilized by Artemis Financial especially if they expand to international exchanges they must have a strong system in place to secure their users sessions to combat hijacking and remote in control.  
Logging and Monitoring: Finally the last area that is critical to the success of Artemis Financial is the logging and monitoring necessary to detect errors, suspicious activities, and breaches with an appropriate response protocol.

# 3. Manual Review

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

1. CRUDController.java the @RequestParam for business\_name does not check data making it vulnerable to SQL Injection and XSS requiring implementation of validation or sanitation.

2. The APIs are vulnerable to unauthorized access due to exposed endpoints including but not limited to /greeting and /read which lack authentication and authorization.

3. There is not utilization of encryption for the sensitive data leaving certain stores like account\_number and account\_blanace exposed as plaintext.

4. The username and password for database connection string are hardcoded in the DocData class creating a high risk for credential exposure that could leak access.

5. There is a code error in the form of e.printStackTrace() in the catch (SQLException e) block of DocData which poses a risk of end users observing the stack traces resulting in a information leak.

6. The int account\_balance field in customer class isn’t private which goes against encapsulation principle and potentially encourages data manipulation.

7. Code quality is lacking as the Java naming rules should consistently remain as example NameSubname.java meaning CRUDController.java and customer.java should be CrudController.java and Customer.java as this promotes disorganization or potential needless replication/confusion.

# 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
* bcprov-jdk15on-1.46.jar
  + 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.
    - CVE-2024-34447 (OSSINDEX) suppress
      1. bouncycastle - Improper Validation of Certificate with Host Mismatch
      2. The software communicates with a host that provides a certificate, but the software does not properly ensure that the certificate is actually associated with that host.
      3. CWE-297 Improper Validation of Certificate with Host Mismatch
      4. CVSSv3:
      5. Base Score: HIGH (7.699999809265137)
      6. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L
      7. References:
      8. OSSINDEX - [CVE-2024-34447] CWE-297: Improper Validation of Certificate with Host Mismatch
      9. OSSIndex - https://www.bouncycastle.org/releasenotes.html#:~:text=CVE%2D2024%2D301XX%20%2D%20When%20endpoint%20identification%20is%20enabled%20in%20the%20BCJSSE%20and%20an%20SSL%20socket%20is%20not%20created%20with%20an%20explicit%20hostname%20(as%20happens%20with%20HttpsURLConnection)%2C%20hostname%20verification%20could%20be%20performed%20against%20a%20DNS%2Dresolved%20IP%20address.%20This%20has%20been%20fixed.
      10. Vulnerable Software & Versions (OSSINDEX):
      11. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
    - CVE-2016-1000338 suppress
      1. In Bouncy Castle JCE Provider version 1.55 and earlier the DSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.
      2. CWE-347 Improper Verification of Cryptographic Signature
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2016-1000338] CWE-347: Improper Verification of Cryptographic Signature
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000338
      12. OSSIndex - https://www.bouncycastle.org/releasenotes.html
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      24. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      25. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      26. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      27. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      28. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      29. Vulnerable Software & Versions: (show all)
      30. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 1.38; versions up to (excluding) 1.56
    - CVE-2016-1000342 suppress
      1. In the Bouncy Castle JCE Provider version 1.55 and earlier ECDSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.
      2. CWE-347 Improper Verification of Cryptographic Signature
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2016-1000342] CWE-347: Improper Verification of Cryptographic Signature
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000342
      12. OSSIndex - https://www.bouncycastle.org/releasenotes.html
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2016-1000343 suppress
      1. 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. If the JCA key pair generator is not explicitly initialised with DSA parameters, 1.55 and earlier generates a private value assuming a 1024 bit key size. In earlier releases this can be dealt with by explicitly passing parameters to the key pair generator.
      2. CWE-310 Cryptographic Issues
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      9. References:
      10. OSSINDEX - [CVE-2016-1000343] CWE-310
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000343
      12. OSSIndex - https://www.bouncycastle.org/releasenotes.html
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2024-29857 (OSSINDEX) suppress
      1. An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castle Java (BC Java) before 1.78, BC Java LTS before 2.73.6, BC-FJA before 1.0.2.5, and BC C# .Net before 2.3.1. Importing an EC certificate with crafted F2m parameters can lead to excessive CPU consumption during the evaluation of the curve parameters.
      2. CWE-125 Out-of-bounds Read
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
      6. References:
      7. OSSINDEX - [CVE-2024-29857] CWE-125: Out-of-bounds Read
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-29857
      9. OSSIndex - https://github.com/advisories/GHSA-8xfc-gm6g-vgpv
      10. OSSIndex - https://www.bouncycastle.org/releasenotes.html#:~:text=the%20following%20CVEs%3A-,CVE%2D2024%2D29857,-%2D%20Importing%20an%20EC
      11. Vulnerable Software & Versions (OSSINDEX):
      12. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
      13. CVE-2016-1000344 suppress
      14. In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.
      15. CWE-310 Cryptographic Issues
      16. CVSSv3:
      17. Base Score: HIGH (7.4)
      18. Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:2.2/RC:R/MAV:A
      19. CVSSv2:
      20. Base Score: MEDIUM (5.8)
      21. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      22. References:
      23. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      24. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. Vulnerable Software & Versions:
      26. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2016-1000352 suppress
      1. In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.
      2. CWE-310 Cryptographic Issues
      3. CVSSv3:
      4. Base Score: HIGH (7.4)
      5. Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      11. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      12. Vulnerable Software & Versions:
      13. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2024-30171 (OSSINDEX) suppress
      1. An issue was discovered in Bouncy Castle Java TLS API and JSSE Provider before 1.78. Timing-based leakage may occur in RSA based handshakes because of exception processing.
      2. CWE-203 Observable Discrepancy
      3. CVSSv3:
      4. Base Score: MEDIUM (5.900000095367432)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
      6. References:
      7. OSSINDEX - [CVE-2024-30171] CWE-203: Information Exposure Through Discrepancy
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-30171
      9. OSSIndex - https://github.com/advisories/GHSA-v435-xc8x-wvr9
      10. OSSIndex - https://github.com/bcgit/bc-java/issues/1528
      11. OSSIndex - https://www.bouncycastle.org/releasenotes.html#:~:text=during%20parameter%20evaluation.-,CVE%2D2024%2D30171,-%2D%20Possible%20timing%20based
      12. Vulnerable Software & Versions (OSSINDEX):
      13. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
    - CVE-2016-1000341 suppress
      1. In the Bouncy Castle JCE Provider version 1.55 and earlier DSA signature generation is vulnerable to timing attack. Where timings can be closely observed for the generation of signatures, the lack of blinding in 1.55, or earlier, may allow an attacker to gain information about the signature's k value and ultimately the private value as well.
      2. CWE-361 7PK - Time and State
      3. CVSSv3:
      4. Base Score: MEDIUM (5.9)
      5. Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. OSSINDEX - [CVE-2016-1000341] CWE-361
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000341
      12. OSSIndex - https://rdist.root.org/2010/11/19/dsa-requirements-for-random-k-value/
      13. OSSIndex - https://www.bouncycastle.org/releasenotes.html
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      17. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions:
      19. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2016-1000345 suppress
      1. In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES/ECIES CBC mode vulnerable to padding oracle attack. For BC 1.55 and older, in an environment where timings can be easily observed, it is possible with enough observations to identify when the decryption is failing due to padding.
      2. CWE-361 7PK - Time and State
      3. CVSSv3:
      4. Base Score: MEDIUM (5.9)
      5. Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. OSSINDEX - [CVE-2016-1000345] CWE-361
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000345
      12. OSSIndex - https://www.bouncycastle.org/releasenotes.html
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2017-13098 suppress
      1. 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. An attacker can recover the private key from a vulnerable application. This vulnerability is referred to as "ROBOT."
      2. CWE-203 Observable Discrepancy
      3. CVSSv3:
      4. Base Score: MEDIUM (5.9)
      5. Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MITIGATION,THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      11. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      16. cret@cert.org - ISSUE\_TRACKING,MITIGATION,THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      17. cret@cert.org - ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      18. cret@cert.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      19. cret@cert.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      20. cret@cert.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      21. cret@cert.org - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      22. Vulnerable Software & Versions:
      23. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.59
    - CVE-2020-15522 suppress
      1. Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math library that can expose information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.
      2. CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
      3. CVSSv3:
      4. Base Score: MEDIUM (5.9)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. cve@mitre.org - RELEASE\_NOTES,VENDOR\_ADVISORY
      14. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      15. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.66
      18. ...
    - CVE-2020-0187 (OSSINDEX) suppress
      1. In engineSetMode of BaseBlockCipher.java, there is a possible incorrect cryptographic algorithm chosen due to an incomplete comparison. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148517383
      2. CWE-Other
      3. CVSSv3:
      4. Base Score: MEDIUM (5.5)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
      6. References:
      7. OSSINDEX - [CVE-2020-0187] CWE-Other
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0187
      9. OSSIndex - https://android.googlesource.com/platform/external/bouncycastle/+/14ceec126e49f2f4748f0d540be820515cc725a6
      10. OSSIndex - https://source.android.com/security/bulletin/pixel/2020-06-01
      11. Vulnerable Software & Versions (OSSINDEX):
      12. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
    - CVE-2023-33202 suppress
      1. Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through the PEMParser causes an OutOfMemoryError, which can enable a denial of service attack. (For users of the FIPS Java API: BC-FJA 1.0.2.3 and earlier are affected; BC-FJA 1.0.2.4 is fixed.)
      2. CWE-400 Uncontrolled Resource Consumption
      3. CVSSv3:
      4. Base Score: MEDIUM (5.5)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:1.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      8. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT
      9. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      10. cve@mitre.org - EXPLOIT,THIRD\_PARTY\_ADVISORY
      11. cve@mitre.org - PRODUCT
      12. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:bouncycastle:bouncy\_castle\_for\_java:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.73
      15. ...
    - CVE-2020-26939 (OSSINDEX) suppress
      1. In Legion of the Bouncy Castle BC before 1.61 and BC-FJA before 1.0.1.2, attackers can obtain sensitive information about a private exponent because of Observable Differences in Behavior to Error Inputs. This occurs in org.bouncycastle.crypto.encodings.OAEPEncoding. Sending invalid ciphertext that decrypts to a short payload in the OAEP Decoder could result in the throwing of an early exception, potentially leaking some information about the private exponent of the RSA private key performing the encryption.
      2. CWE-203 Observable Discrepancy
      3. CVSSv3:
      4. Base Score: MEDIUM (5.300000190734863)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
      6. References:
      7. OSSINDEX - [CVE-2020-26939] CWE-203: Information Exposure Through Discrepancy
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-26939
      9. OSSIndex - https://github.com/bcgit/bc-java/wiki/CVE-2020-26939
      10. Vulnerable Software & Versions (OSSINDEX):
      11. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
    - CVE-2023-33201 (OSSINDEX) suppress
      1. Bouncy Castle For Java before 1.74 is affected by an LDAP injection vulnerability. The vulnerability only affects applications that use an LDAP CertStore from Bouncy Castle to validate X.509 certificates. During the certificate validation process, Bouncy Castle inserts the certificate's Subject Name into an LDAP search filter without any escaping, which leads to an LDAP injection vulnerability.
      2. CWE-295 Improper Certificate Validation
      3. CVSSv3:
      4. Base Score: MEDIUM (5.300000190734863)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
      6. References:
      7. OSSINDEX - [CVE-2023-33201] CWE-295: Improper Certificate Validation
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-33201
      9. OSSIndex - https://github.com/bcgit/bc-java/wiki/CVE-2023-33201
      10. Vulnerable Software & Versions (OSSINDEX):
      11. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
    - CVE-2016-1000339 suppress
      1. In the Bouncy Castle JCE Provider version 1.55 and earlier the primary engine class used for AES was AESFastEngine. Due to the highly table driven approach used in the algorithm it turns out that if the data channel on the CPU can be monitored the lookup table accesses are sufficient to leak information on the AES key being used. There was also a leak in AESEngine although it was substantially less. AESEngine has been modified to remove any signs of leakage (testing carried out on Intel X86-64) and is now the primary AES class for the BC JCE provider from 1.56. Use of AESFastEngine is now only recommended where otherwise deemed appropriate.
      2. CWE-310 Cryptographic Issues
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      14. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      15. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions:
      17. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2015-7940 suppress
      1. The Bouncy Castle Java library before 1.51 does not validate a point is withing the elliptic curve, which makes it easier for remote attackers to obtain private keys via a series of crafted elliptic curve Diffie Hellman (ECDH) key exchanges, aka an "invalid curve attack."
      2. CWE-200 Exposure of Sensitive Information to an Unauthorized Actor, CWE-310 Cryptographic Issues
      3. CVSSv2:
      4. Base Score: MEDIUM (5.0)
      5. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      6. References:
      7. OSSINDEX - [CVE-2015-7940] CWE-200: Information Exposure
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7940
      9. OSSIndex - https://bugzilla.redhat.com/show\_bug.cgi?id=1276272
      10. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      15. cve@mitre.org - TECHNICAL\_DESCRIPTION
      16. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      17. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      18. cve@mitre.org - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      19. cve@mitre.org - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:bouncycastle:bouncy\_castle\_crypto\_package:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.50
      22. ...
    - CVE-2018-5382 suppress
      1. 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. 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. It should be noted that the use of "BKS-V1" is discouraged by the library authors and should only be used where it is otherwise safe to do so, as in where the use of a 16 bit checksum for the file integrity check is not going to cause a security issue in itself.
      2. CWE-327 Use of a Broken or Risky Cryptographic Algorithm, CWE-354 Improper Validation of Integrity Check Value
      3. CVSSv3:
      4. Base Score: MEDIUM (4.4)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2018-5382] CWE-327: Use of a Broken or Risky Cryptographic Algorithm
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5382
      12. OSSIndex - https://blog.sonatype.com/cve-2018-2018-5382-bouncycastle-information-exposure
      13. OSSIndex - https://insights.sei.cmu.edu/cert/2018/03/the-curious-case-of-the-bouncy-castle-bks-passwords.html
      14. OSSIndex - https://www.bouncycastle.org/releasenotes.html
      15. OSSIndex - https://www.kb.cert.org/vuls/id/306792
      16. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,VENDOR\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      21. cret@cert.org - RELEASE\_NOTES,VENDOR\_ADVISORY
      22. cret@cert.org - THIRD\_PARTY\_ADVISORY
      23. cret@cert.org - THIRD\_PARTY\_ADVISORY
      24. cret@cert.org - THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      25. cret@cert.org - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      26. Vulnerable Software & Versions: (show all)
      27. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.49
      28. ...
    - CVE-2013-1624 suppress
      1. 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.
      2. CWE-310 Cryptographic Issues
      3. CVSSv2:
      4. Base Score: MEDIUM (4.0)
      5. Vector: /AV:N/AC:H/Au:N/C:P/I:P/A:N
      6. References:
      7. OSSINDEX - [CVE-2013-1624] CWE-310
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1624
      9. OSSIndex - https://bugzilla.redhat.com/show\_bug.cgi?id=908428
      10. Vulnerable Software & Versions: (show all)
      11. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\*
      12. ...
    - CVE-2016-1000346 suppress
      1. 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. As of release 1.56 the key parameters are checked on agreement calculation.
      2. CWE-320 Key Management Errors
      3. CVSSv3:
      4. Base Score: LOW (3.7)
      5. Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. OSSINDEX - [CVE-2016-1000346] CWE-320
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000346
      12. OSSIndex - https://news.ycombinator.com/item?id=7959519
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.55
    - CVE-2015-6644 (OSSINDEX) suppress
      1. Bouncy Castle in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information via a crafted application, aka internal bug 24106146.
      2. CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: LOW (3.299999952316284)
      5. Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
      6. References:
      7. OSSINDEX - [CVE-2015-6644] CWE-200: Information Exposure
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6644
      9. OSSIndex - https://bugzilla.redhat.com/show\_bug.cgi?id=1444015
      10. OSSIndex - https://github.com/bcgit/bc-java/issues/177
      11. Vulnerable Software & Versions (OSSINDEX):
      12. cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:\*:\*:\*:\*:\*:\*:\*
* hibernate-validator-6.0.18.Final.jar
  + Hibernate's Bean Validation (JSR-380) reference implementation.
    - CVE-2023-1932 (OSSINDEX) suppress
      1. A flaw was found in hibernate-validator's 'isValid' method in the org.hibernate.validator.internal.constraintvalidators.hv.SafeHtmlValidator class, which can be bypassed by omitting the tag ending in a less-than character. Browsers may render an invalid html, allowing HTML injection or Cross-Site-Scripting (XSS) attacks.
      2. Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2023-1932 for details
      3. CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
      4. CVSSv2:
      5. Base Score: MEDIUM (5.300000190734863)
      6. Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
      7. References:
      8. OSSINDEX - [CVE-2023-1932] CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
      9. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1932
      10. OSSIndex - https://github.com/advisories/GHSA-x83m-pf6f-pf9g
      11. Vulnerable Software & Versions (OSSINDEX):
      12. cpe:2.3:a:org.hibernate.validator:hibernate-validator:6.0.18.Final:\*:\*:\*:\*:\*:\*:\*
    - CVE-2020-10693 suppress
      1. 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.
      2. CWE-20 Improper Input Validation
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2020-10693] CWE-20: Improper Input Validation
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693
      12. OSSIndex - https://github.com/hibernate/hibernate-validator/pull/1092
      13. OSSIndex - https://github.com/hibernate/hibernate-validator/pull/1093
      14. OSSIndex - https://github.com/hibernate/hibernate-validator/pull/1094
      15. OSSIndex - https://hibernate.atlassian.net/browse/HV-1774
      16. OSSIndex - https://in.relation.to/2020/05/07/hibernate-validator-615-6020-released/
      17. OSSIndex - https://openliberty.io/docs/latest/security-vulnerabilities.html
      18. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      20. secalert@redhat.com - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      21. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      22. Vulnerable Software & Versions: (show all)
      23. cpe:2.3:a:redhat:hibernate\_validator:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.0.0; versions up to (excluding) 6.0.20
      24. ...
* jackson-databind-2.10.2.jar
  + General data-binding functionality for Jackson: works on core streaming API
    - CVE-2020-25649 suppress
      1. A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.
      2. CWE-611 Improper Restriction of XML External Entity Reference
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2020-25649] CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649
      12. OSSIndex - https://github.com/FasterXML/jackson-databind/issues/2589
      13. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. secalert@redhat.com - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      23. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      24. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      25. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      26. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      27. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      28. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      29. secalert@redhat.com - PATCH,THIRD\_PARTY\_ADVISORY
      30. secalert@redhat.com - THIRD\_PARTY\_ADVISORY
      31. Vulnerable Software & Versions: (show all)
      32. cpe:2.3:a:fasterxml:jackson-databind:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 2.10.0; versions up to (excluding) 2.10.5.1
      33. ...
    - CVE-2020-36518 suppress
      1. jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.
      2. CWE-787 Out-of-bounds Write
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. OSSINDEX - [CVE-2020-36518] CWE-787: Out-of-bounds Write
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-36518
      12. OSSIndex - https://github.com/FasterXML/jackson-databind/issues/2816
      13. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. cve@mitre.org - EXPLOIT,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      22. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      23. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      24. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      25. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      26. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      27. Vulnerable Software & Versions: (show all)
      28. cpe:2.3:a:fasterxml:jackson-databind:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.12.6.1
      29. ...
    - CVE-2021-46877 suppress
      1. jackson-databind 2.10.x through 2.12.x before 2.12.6 and 2.13.x before 2.13.1 allows attackers to cause a denial of service (2 GB transient heap usage per read) in uncommon situations involving JsonNode JDK serialization.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2021-46877] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      8. OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3328
      9. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,VENDOR\_ADVISORY
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES
      11. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,VENDOR\_ADVISORY
      12. cve@mitre.org - MAILING\_LIST,RELEASE\_NOTES
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:fasterxml:jackson-databind:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 2.10.0; versions up to (excluding) 2.12.6
      15. ...
    - CVE-2022-42003 suppress
      1. In FasterXML jackson-databind before versions 2.13.4.1 and 2.12.17.1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP\_SINGLE\_VALUE\_ARRAYS feature is enabled.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-42003] CWE-502: Deserialization of Untrusted Data
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42003
      9. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020
      10. OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3590
      11. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      19. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      20. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      22. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      23. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      24. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      25. Vulnerable Software & Versions: (show all)
      26. cpe:2.3:a:fasterxml:jackson-databind:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.12.7.1
      27. ...
    - CVE-2022-42004 suppress
      1. In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer.\_deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-42004] CWE-502: Deserialization of Untrusted Data
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42004
      9. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490
      10. OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3582
      11. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      19. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      20. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      22. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      23. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      24. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      25. Vulnerable Software & Versions: (show all)
      26. cpe:2.3:a:fasterxml:jackson-databind:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.12.7.1
      27. ...
    - CVE-2023-35116 suppress
      1. jackson-databind through 2.15.2 allows attackers to cause a denial of service or other unspecified impact via a crafted object that uses cyclic dependencies. NOTE: the vendor's perspective is that this is not a valid vulnerability report, because the steps of constructing a cyclic data structure and trying to serialize it cannot be achieved by an external attacker.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (4.7)
      5. Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.0/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      8. cve@mitre.org - ISSUE\_TRACKING
      9. Vulnerable Software & Versions:
      10. cpe:2.3:a:fasterxml:jackson-databind:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.16.0
* log4j-api-2.12.1.jar
  + The Apache Log4j API
    - CVE-2020-9488 suppress
      1. 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
      2. CWE-295 Improper Certificate Validation
      3. CVSSv3:
      4. Base Score: LOW (3.7)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MITIGATION,PATCH,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - ISSUE\_TRACKING,MITIGATION,PATCH,VENDOR\_ADVISORY
      21. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. Vulnerable Software & Versions: (show all)
      31. cpe:2.3:a:apache:log4j:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 2.4; versions up to (excluding) 2.12.3
      32. ...
* logback-classic-1.2.3.jar
  + logback-classic module
    - CVE-2023-6378 suppress
      1. A serialization vulnerability in logback receiver component part of
      2. logback version 1.4.11 allows an attacker to mount a Denial-Of-Service
      3. attack by sending poisoned data.
      4. CWE-502 Deserialization of Untrusted Data
      5. CVSSv3:
      6. Base Score: HIGH (7.5)
      7. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      8. References:
      9. OSSINDEX - [CVE-2023-6378] CWE-502: Deserialization of Untrusted Data
      10. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-6378
      11. OSSIndex - https://github.com/advisories/GHSA-vmq6-5m68-f53m
      12. OSSIndex - https://logback.qos.ch/news.html#1.3.12
      13. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      14. vulnerability@ncsc.ch - RELEASE\_NOTES
      15. Vulnerable Software & Versions: (show all)
      16. cpe:2.3:a:qos:logback:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 1.2.0; versions up to (excluding) 1.2.13
      17. ...
    - CVE-2021-42550 suppress
      1. 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.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: MEDIUM (6.6)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:0.7/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: HIGH (8.5)
      8. Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C
      9. References:
      10. OSSINDEX - [CVE-2021-42550] CWE-502: Deserialization of Untrusted Data
      11. OSSIndex - https://jira.qos.ch/browse/LOGBACK-1591
      12. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      15. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      19. vulnerability@ncsc.ch - EXPLOIT,ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      20. vulnerability@ncsc.ch - EXPLOIT,THIRD\_PARTY\_ADVISORY
      21. vulnerability@ncsc.ch - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      22. vulnerability@ncsc.ch - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      23. vulnerability@ncsc.ch - THIRD\_PARTY\_ADVISORY
      24. vulnerability@ncsc.ch - THIRD\_PARTY\_ADVISORY
      25. vulnerability@ncsc.ch - VENDOR\_ADVISORY
      26. Vulnerable Software & Versions: (show all)
      27. cpe:2.3:a:qos:logback:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.2.7
      28. ...
* logback-core-1.2.3.jar
  + logback-core module
    - CVE-2023-6378 suppress
      1. A serialization vulnerability in logback receiver component part of
      2. logback version 1.4.11 allows an attacker to mount a Denial-Of-Service
      3. attack by sending poisoned data.
      4. CWE-502 Deserialization of Untrusted Data
      5. CVSSv3:
      6. Base Score: HIGH (7.5)
      7. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      8. References:
      9. OSSINDEX - [CVE-2023-6378] CWE-502: Deserialization of Untrusted Data
      10. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-6378
      11. OSSIndex - https://github.com/advisories/GHSA-vmq6-5m68-f53m
      12. OSSIndex - https://logback.qos.ch/news.html#1.3.12
      13. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      14. vulnerability@ncsc.ch - RELEASE\_NOTES
      15. Vulnerable Software & Versions: (show all)
      16. cpe:2.3:a:qos:logback:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 1.2.0; versions up to (excluding) 1.2.13
      17. ...
    - CVE-2021-42550 suppress
      1. 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.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: MEDIUM (6.6)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:0.7/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: HIGH (8.5)
      8. Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C
      9. References:
      10. OSSINDEX - [CVE-2021-42550] CWE-502: Deserialization of Untrusted Data
      11. OSSIndex - https://jira.qos.ch/browse/LOGBACK-1591
      12. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      15. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      19. vulnerability@ncsc.ch - EXPLOIT,ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      20. vulnerability@ncsc.ch - EXPLOIT,THIRD\_PARTY\_ADVISORY
      21. vulnerability@ncsc.ch - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      22. vulnerability@ncsc.ch - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      23. vulnerability@ncsc.ch - THIRD\_PARTY\_ADVISORY
      24. vulnerability@ncsc.ch - THIRD\_PARTY\_ADVISORY
      25. vulnerability@ncsc.ch - VENDOR\_ADVISORY
      26. Vulnerable Software & Versions: (show all)
      27. cpe:2.3:a:qos:logback:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 1.2.7
      28. ...
* snakeyaml-1.25.jar
  + YAML 1.1 parser and emitter for Java
    - CVE-2022-1471 suppress
      1. SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.
      2. CWE-502 Deserialization of Untrusted Data, CWE-20 Improper Input Validation
      3. CVSSv3:
      4. Base Score: CRITICAL (9.8)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-1471] CWE-20: Improper Input Validation
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1471
      9. OSSIndex - https://github.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2
      10. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      14. cve-coordination@google.com - EXPLOIT,THIRD\_PARTY\_ADVISORY
      15. cve-coordination@google.com - EXPLOIT,THIRD\_PARTY\_ADVISORY
      16. cve-coordination@google.com - EXPLOIT,THIRD\_PARTY\_ADVISORY
      17. cve-coordination@google.com - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions:
      19. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.0
      20. CVE-2017-18640 suppress
      21. The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564.
      22. CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
      23. CVSSv3:
      24. Base Score: HIGH (7.5)
      25. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      26. CVSSv2:
      27. Base Score: MEDIUM (5.0)
      28. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      29. References:
      30. OSSINDEX - [CVE-2017-18640] CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
      31. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640
      32. OSSIndex - https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion
      33. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      34. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      35. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      36. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      37. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      38. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      39. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,PATCH,THIRD\_PARTY\_ADVISORY
      40. cve@mitre.org - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      41. cve@mitre.org - PATCH,THIRD\_PARTY\_ADVISORY
      42. cve@mitre.org - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      43. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      44. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      45. Vulnerable Software & Versions: (show all)
      46. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.26
      47. ...
    - CVE-2022-25857 suppress
      1. 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.
      2. CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-25857] CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-25857
      9. OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/525
      10. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. report@snyk.io - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      16. report@snyk.io - EXPLOIT,PATCH,THIRD\_PARTY\_ADVISORY
      17. report@snyk.io - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      18. report@snyk.io - PATCH,THIRD\_PARTY\_ADVISORY
      19. report@snyk.io - PATCH,THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions:
      21. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.31
    - CVE-2022-38749 suppress
      1. Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.
      2. CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-38749] CWE-121: Stack-based Buffer Overflow
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38749
      9. OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/525
      10. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47024
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. cve-coordination@google.com - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      15. cve-coordination@google.com - THIRD\_PARTY\_ADVISORY
      16. cve-coordination@google.com - THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.31
    - CVE-2022-38751 suppress
      1. Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.
      2. CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-38751] CWE-121: Stack-based Buffer Overflow
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38751
      9. OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/530/stackoverflow-oss-fuzz-47039
      10. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47039
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. cve-coordination@google.com - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      15. cve-coordination@google.com - THIRD\_PARTY\_ADVISORY
      16. cve-coordination@google.com - THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.31
    - CVE-2022-38752 suppress
      1. Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack-overflow.
      2. CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-38752] CWE-121: Stack-based Buffer Overflow
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38752
      9. OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/531/stackoverflow-oss-fuzz-47081
      10. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47081
      11. OSSIndex - https://github.com/advisories/GHSA-9w3m-gqgf-c4p9
      12. af854a3a-2127-422b-91ae-364da2661108 - PERMISSIONS\_REQUIRED
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. cve-coordination@google.com - PERMISSIONS\_REQUIRED
      15. cve-coordination@google.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions:
      17. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.32
    - CVE-2022-41854 suppress
      1. Those using Snakeyaml to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack overflow. This effect may support a denial of service attack.
      2. CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-41854] CWE-121: Stack-based Buffer Overflow
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-41854
      9. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355
      10. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      11. cve-coordination@google.com - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      12. Vulnerable Software & Versions:
      13. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.32
    - CVE-2022-38750 suppress
      1. Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.
      2. CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow
      3. CVSSv3:
      4. Base Score: MEDIUM (5.5)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:1.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2022-38750] CWE-121: Stack-based Buffer Overflow
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38750
      9. OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/526/stackoverflow-oss-fuzz-47027
      10. OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47027
      11. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. cve-coordination@google.com - EXPLOIT,ISSUE\_TRACKING,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      15. cve-coordination@google.com - EXPLOIT,ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      16. cve-coordination@google.com - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:snakeyaml\_project:snakeyaml:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 1.31
* spring-boot-2.2.4.RELEASE.jar
  + Spring Boot
    - CVE-2023-20873 suppress
      1. In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: CRITICAL (9.8)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      8. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      9. security@vmware.com - THIRD\_PARTY\_ADVISORY
      10. security@vmware.com - VENDOR\_ADVISORY
      11. Vulnerable Software & Versions: (show all)
      12. cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.5.15
      13. ...
    - CVE-2022-27772 suppress
      1. 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
      2. CWE-668 Exposure of Resource to Wrong Sphere
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. OSSINDEX - [CVE-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772
      12. OSSIndex - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
      13. OSSIndex - https://github.com/github/codeql/pull/4473#issuecomment-1030416237
      14. OSSIndex - https://github.com/spring-projects/spring-boot/issues/23622
      15. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,PATCH,THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - EXPLOIT,PATCH,THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.2.11
    - CVE-2023-20883 suppress
      1. In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.
      2. CWE-400 Uncontrolled Resource Consumption
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      8. security@vmware.com - VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.5.14
      11. ...
* spring-boot-starter-web-2.2.4.RELEASE.jar
  + Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container
    - CVE-2023-20873 suppress
      1. In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: CRITICAL (9.8)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      8. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      9. security@vmware.com - THIRD\_PARTY\_ADVISORY
      10. security@vmware.com - VENDOR\_ADVISORY
      11. Vulnerable Software & Versions: (show all)
      12. cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.5.15
      13. ...
    - CVE-2022-27772 suppress
      1. 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
      2. CWE-668 Exposure of Resource to Wrong Sphere
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. OSSINDEX - [CVE-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772
      12. OSSIndex - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
      13. OSSIndex - https://github.com/github/codeql/pull/4473#issuecomment-1030416237
      14. OSSIndex - https://github.com/spring-projects/spring-boot/issues/23622
      15. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,PATCH,THIRD\_PARTY\_ADVISORY
      16. cve@mitre.org - EXPLOIT,PATCH,THIRD\_PARTY\_ADVISORY
      17. Vulnerable Software & Versions:
      18. cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.2.11
    - CVE-2023-20883 suppress
      1. In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.
      2. CWE-400 Uncontrolled Resource Consumption
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      8. security@vmware.com - VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:vmware:spring\_boot:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 2.5.14
      11. ...
* spring-core-5.2.3.RELEASE.jar
  + Spring Core
    - CVE-2022-22965 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: VMware Spring Framework
      3. Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
      4. Date Added: 2022-04-04
      5. Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
      6. Required Action: Apply updates per vendor instructions.
      7. Due Date: 2022-04-25
      8. Notes: https://nvd.nist.gov/vuln/detail/CVE-2022-22965
      9. 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.
      10. CWE-94 Improper Control of Generation of Code ('Code Injection')
      11. CVSSv3:
      12. Base Score: CRITICAL (9.8)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      14. CVSSv2:
      15. Base Score: HIGH (7.5)
      16. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      17. References:
      18. OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
      19. OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest\_sys/status/1509053689331335174
      20. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
      21. OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
      22. OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
      23. OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
      24. OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/
      25. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      26. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      27. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      28. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      29. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      30. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      31. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      32. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      33. security@vmware.com - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      34. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      35. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      36. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      37. security@vmware.com - THIRD\_PARTY\_ADVISORY
      38. security@vmware.com - THIRD\_PARTY\_ADVISORY
      39. security@vmware.com - THIRD\_PARTY\_ADVISORY
      40. security@vmware.com - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      41. Vulnerable Software & Versions: (show all)
      42. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      43. ...
    - CVE-2021-22118 suppress
      1. In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.
      2. CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      18. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      19. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      20. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      21. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@vmware.com - THIRD\_PARTY\_ADVISORY
      23. security@vmware.com - THIRD\_PARTY\_ADVISORY
      24. Vulnerable Software & Versions: (show all)
      25. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.15
      26. ...
    - CVE-2020-5421 suppress
      1. In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.6)
      8. Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      18. security@pivotal.io - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      19. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      20. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      21. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@pivotal.io - THIRD\_PARTY\_ADVISORY
      25. security@pivotal.io - VENDOR\_ADVISORY
      26. Vulnerable Software & Versions: (show all)
      27. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.9
      28. ...
    - CVE-2022-22950 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      12. Vulnerable Software & Versions: (show all)
      13. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      14. ...
    - CVE-2022-22971 suppress
      1. 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. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.21
      18. ...
    - CVE-2023-20861 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      8. security@vmware.com - VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.22
      11. ...
    - CVE-2023-20863 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      8. security@vmware.com - VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
      11. ...
    - CVE-2022-22968 suppress
      1. 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.
      2. CWE-178 Improper Handling of Case Sensitivity
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      13. security@vmware.com - THIRD\_PARTY\_ADVISORY
      14. security@vmware.com - THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - VENDOR\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.20
      18. ...
    - CVE-2022-22970 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.5)
      8. Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.21
      18. ...
    - CVE-2021-22060 suppress
      1. 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2021-22060] CWE-noinfo
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060
      12. OSSIndex - https://tanzu.vmware.com/security/cve-2021-22060
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. security@vmware.com - VENDOR\_ADVISORY
      17. Vulnerable Software & Versions: (show all)
      18. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.18
      19. ...
    - CVE-2021-22096 suppress
      1. In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.
      2. CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      13. security@vmware.com - THIRD\_PARTY\_ADVISORY
      14. security@vmware.com - THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - VENDOR\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.17
      18. ...
* spring-expression-5.2.3.RELEASE.jar
  + Spring Expression Language (SpEL)
    - CVE-2022-22965 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: VMware Spring Framework
      3. Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
      4. Date Added: 2022-04-04
      5. Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
      6. Required Action: Apply updates per vendor instructions.
      7. Due Date: 2022-04-25
      8. Notes: https://nvd.nist.gov/vuln/detail/CVE-2022-22965
      9. 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.
      10. CWE-94 Improper Control of Generation of Code ('Code Injection')
      11. CVSSv3:
      12. Base Score: CRITICAL (9.8)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      14. CVSSv2:
      15. Base Score: HIGH (7.5)
      16. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      17. References:
      18. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      19. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      25. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      26. security@vmware.com - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      27. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      28. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      29. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      30. security@vmware.com - THIRD\_PARTY\_ADVISORY
      31. security@vmware.com - THIRD\_PARTY\_ADVISORY
      32. security@vmware.com - THIRD\_PARTY\_ADVISORY
      33. security@vmware.com - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      34. Vulnerable Software & Versions: (show all)
      35. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      36. ...
    - CVE-2021-22118 suppress
      1. In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.
      2. CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. OSSINDEX - [CVE-2021-22118] CWE-269: Improper Privilege Management
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118
      12. OSSIndex - https://github.com/spring-projects/spring-framework/issues/26931
      13. OSSIndex - https://tanzu.vmware.com/security/cve-2021-22118
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@vmware.com - THIRD\_PARTY\_ADVISORY
      27. security@vmware.com - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.15
      30. ...
    - CVE-2020-5421 suppress
      1. In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.6)
      8. Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2020-5421] CWE-noinfo
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421
      12. OSSIndex - https://tanzu.vmware.com/security/cve-2020-5421
      13. af854a3a-2127-422b-91ae-364da2661108 - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      21. security@pivotal.io - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      22. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      27. security@pivotal.io - THIRD\_PARTY\_ADVISORY
      28. security@pivotal.io - VENDOR\_ADVISORY
      29. Vulnerable Software & Versions: (show all)
      30. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.9
      31. ...
    - CVE-2022-22950 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. OSSINDEX - [CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950
      12. OSSIndex - https://github.com/spring-projects/spring-framework/issues/28145
      13. OSSIndex - https://spring.io/blog/2022/03/17/spring-framework-6-0-0-m3-and-5-3-17-available-now
      14. OSSIndex - https://tanzu.vmware.com/security/cve-2022-22950
      15. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      16. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      17. Vulnerable Software & Versions: (show all)
      18. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      19. ...
    - CVE-2022-22971 suppress
      1. 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. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.21
      18. ...
    - CVE-2023-20861 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2023-20861] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861
      9. OSSIndex - https://spring.io/blog/2023/03/20/spring-framework-5-2-23-fixes-cve-2023-20861
      10. OSSIndex - https://spring.io/security/cve-2023-20861
      11. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      12. security@vmware.com - VENDOR\_ADVISORY
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.22
      15. ...
    - CVE-2023-20863 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2023-20863] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863
      9. OSSIndex - https://github.com/spring-projects/spring-framework/issues/30325
      10. OSSIndex - https://spring.io/security/cve-2023-20863
      11. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      12. security@vmware.com - VENDOR\_ADVISORY
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
      15. ...
    - CVE-2024-38808 (OSSINDEX) suppress
      1. In Spring Framework versions 5.3.0 - 5.3.38 and older unsupported versions, it is possible for a user to provide a specially crafted Spring Expression Language (SpEL) expression that may cause a denial of service (DoS) condition.
      2. Specifically, an application is vulnerable when the following is true:
      3. \* The application evaluates user-supplied SpEL expressions.
      4. Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2024-38808 for details
      5. CWE-770 Allocation of Resources Without Limits or Throttling
      6. CVSSv2:
      7. Base Score: MEDIUM (5.300000190734863)
      8. Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
      9. References:
      10. OSSINDEX - [CVE-2024-38808] CWE-770: Allocation of Resources Without Limits or Throttling
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38808
      12. OSSIndex - https://spring.io/security/cve-2024-38808
      13. Vulnerable Software & Versions (OSSINDEX):
      14. cpe:2.3:a:org.springframework:spring-expression:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*
    - CVE-2022-22968 suppress
      1. 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.
      2. CWE-178 Improper Handling of Case Sensitivity
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
      12. OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
      13. OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
      14. OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
      15. OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      19. security@vmware.com - THIRD\_PARTY\_ADVISORY
      20. security@vmware.com - THIRD\_PARTY\_ADVISORY
      21. security@vmware.com - VENDOR\_ADVISORY
      22. Vulnerable Software & Versions: (show all)
      23. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.20
      24. ...
    - CVE-2022-22970 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.5)
      8. Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.21
      18. ...
    - CVE-2021-22060 suppress
      1. 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      12. security@vmware.com - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - VENDOR\_ADVISORY
      14. Vulnerable Software & Versions: (show all)
      15. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.18
      16. ...
      17. CVE-2021-22096 suppress
      18. In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.
      19. CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other
      20. CVSSv3:
      21. Base Score: MEDIUM (4.3)
      22. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      23. CVSSv2:
      24. Base Score: MEDIUM (4.0)
      25. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      26. References:
      27. OSSINDEX - [CVE-2021-22096] CWE-117: Improper Output Neutralization for Logs
      28. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096
      29. OSSIndex - https://tanzu.vmware.com/security/cve-2021-22096
      30. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      31. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      32. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      33. security@vmware.com - THIRD\_PARTY\_ADVISORY
      34. security@vmware.com - THIRD\_PARTY\_ADVISORY
      35. security@vmware.com - VENDOR\_ADVISORY
      36. Vulnerable Software & Versions: (show all)
      37. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.17
      38. ...
* spring-web-5.2.3.RELEASE.jar
  + Spring Web
    - CVE-2016-1000027 suppress
      1. 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.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: CRITICAL (9.8)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: HIGH (7.5)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. OSSINDEX - [CVE-2016-1000027] CWE-502: Deserialization of Untrusted Data
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027
      12. OSSIndex - https://blog.gypsyengineer.com/en/security/detecting-dangerous-spring-exporters-with-codeql.html
      13. OSSIndex - https://bugzilla.redhat.com/show\_bug.cgi?id=CVE-2016-1000027
      14. OSSIndex - https://github.com/spring-projects/spring-framework/issues/24434
      15. OSSIndex - https://www.tenable.com/security/research/tra-2016-20
      16. af854a3a-2127-422b-91ae-364da2661108 - BROKEN\_LINK,EXPLOIT,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. cve@mitre.org - BROKEN\_LINK,EXPLOIT,THIRD\_PARTY\_ADVISORY
      25. cve@mitre.org - EXPLOIT,THIRD\_PARTY\_ADVISORY
      26. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      27. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      28. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      29. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      30. cve@mitre.org - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      31. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      32. Vulnerable Software & Versions:
      33. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 6.0.0
    - CVE-2022-22965 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: VMware Spring Framework
      3. Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
      4. Date Added: 2022-04-04
      5. Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
      6. Required Action: Apply updates per vendor instructions.
      7. Due Date: 2022-04-25
      8. Notes: https://nvd.nist.gov/vuln/detail/CVE-2022-22965
      9. 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.
      10. CWE-94 Improper Control of Generation of Code ('Code Injection')
      11. CVSSv3:
      12. Base Score: CRITICAL (9.8)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      14. CVSSv2:
      15. Base Score: HIGH (7.5)
      16. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      17. References:
      18. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      19. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      25. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      26. security@vmware.com - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      27. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      28. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      29. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      30. security@vmware.com - THIRD\_PARTY\_ADVISORY
      31. security@vmware.com - THIRD\_PARTY\_ADVISORY
      32. security@vmware.com - THIRD\_PARTY\_ADVISORY
      33. security@vmware.com - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      34. Vulnerable Software & Versions: (show all)
      35. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      36. ...
    - CVE-2024-38809 (OSSINDEX) suppress
      1. Applications that parse ETags from "If-Match" or "If-None-Match" request headers are vulnerable to DoS attack.
      2. Users of affected versions should upgrade to the corresponding fixed version.
      3. Users of older, unsupported versions could enforce a size limit on "If-Match" and "If-None-Match" headers, e.g. through a Filter.
      4. CWE-400 Uncontrolled Resource Consumption
      5. CVSSv2:
      6. Base Score: HIGH (8.699999809265137)
      7. Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
      8. References:
      9. OSSINDEX - [CVE-2024-38809] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      10. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38809
      11. OSSIndex - https://spring.io/security/cve-2024-38809
      12. Vulnerable Software & Versions (OSSINDEX):
      13. cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*
    - CVE-2024-22243 (OSSINDEX) suppress
      1. Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks.
      2. Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2024-22243 for details
      3. CWE-601 URL Redirection to Untrusted Site ('Open Redirect')
      4. CVSSv3:
      5. Base Score: HIGH (8.100000381469727)
      6. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
      7. References:
      8. OSSINDEX - [CVE-2024-22243] CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
      9. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22243
      10. OSSIndex - https://github.com/spring-projects/spring-framework/issues/32211
      11. OSSIndex - https://spring.io/security/cve-2024-22243
      12. Vulnerable Software & Versions (OSSINDEX):
      13. cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*
    - CVE-2024-22262 (OSSINDEX) suppress
      1. Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks.
      2. This is the same as CVE-2024-22259 https://spring.io/security/cve-2024-22259 and CVE-2024-22243 https://spring.io/security/cve-2024-22243 , but with different input.
      3. CWE-601 URL Redirection to Untrusted Site ('Open Redirect')
      4. CVSSv3:
      5. Base Score: HIGH (8.100000381469727)
      6. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
      7. References:
      8. OSSINDEX - [CVE-2024-22262] CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
      9. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22262
      10. OSSIndex - https://github.com/spring-projects/spring-framework/issues/32616
      11. OSSIndex - https://spring.io/security/cve-2024-22262
      12. Vulnerable Software & Versions (OSSINDEX):
      13. cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*
    - CVE-2021-22118 suppress
      1. In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.
      2. CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. OSSINDEX - [CVE-2021-22118] CWE-269: Improper Privilege Management
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118
      12. OSSIndex - https://github.com/spring-projects/spring-framework/issues/26931
      13. OSSIndex - https://tanzu.vmware.com/security/cve-2021-22118
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@vmware.com - THIRD\_PARTY\_ADVISORY
      27. security@vmware.com - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.15
      30. ...
    - CVE-2024-38828 (OSSINDEX) suppress
      1. Spring MVC controller methods with an @RequestBody byte[] method parameter are vulnerable to a DoS attack.
      2. CWE-400 Uncontrolled Resource Consumption
      3. CVSSv2:
      4. Base Score: MEDIUM (6.900000095367432)
      5. Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
      6. References:
      7. OSSINDEX - [CVE-2024-38828] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38828
      9. OSSIndex - https://spring.io/blog/2024/11/15/spring-framework-cve-2024-38828-published
      10. OSSIndex - https://spring.io/security/cve-2024-38828
      11. Vulnerable Software & Versions (OSSINDEX):
      12. cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*
    - CVE-2020-5421 suppress
      1. In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.6)
      8. Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2020-5421] CWE-noinfo
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421
      12. OSSIndex - https://tanzu.vmware.com/security/cve-2020-5421
      13. af854a3a-2127-422b-91ae-364da2661108 - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      21. security@pivotal.io - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      22. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      27. security@pivotal.io - THIRD\_PARTY\_ADVISORY
      28. security@pivotal.io - VENDOR\_ADVISORY
      29. Vulnerable Software & Versions: (show all)
      30. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.9
      31. ...
    - CVE-2022-22950 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. OSSINDEX - [CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950
      12. OSSIndex - https://github.com/spring-projects/spring-framework/issues/28145
      13. OSSIndex - https://spring.io/blog/2022/03/17/spring-framework-6-0-0-m3-and-5-3-17-available-now
      14. OSSIndex - https://tanzu.vmware.com/security/cve-2022-22950
      15. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      16. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      17. Vulnerable Software & Versions: (show all)
      18. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      19. ...
    - CVE-2022-22971 suppress
      1. 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. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.21
      18. ...
    - CVE-2023-20861 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2023-20861] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861
      9. OSSIndex - https://spring.io/blog/2023/03/20/spring-framework-5-2-23-fixes-cve-2023-20861
      10. OSSIndex - https://spring.io/security/cve-2023-20861
      11. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      12. security@vmware.com - VENDOR\_ADVISORY
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.22
      15. ...
    - CVE-2023-20863 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. OSSINDEX - [CVE-2023-20863] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
      8. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863
      9. OSSIndex - https://github.com/spring-projects/spring-framework/issues/30325
      10. OSSIndex - https://spring.io/security/cve-2023-20863
      11. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      12. security@vmware.com - VENDOR\_ADVISORY
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
      15. ...
    - CVE-2022-22968 suppress
      1. 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.
      2. CWE-178 Improper Handling of Case Sensitivity
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
      12. OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
      13. OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
      14. OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
      15. OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      19. security@vmware.com - THIRD\_PARTY\_ADVISORY
      20. security@vmware.com - THIRD\_PARTY\_ADVISORY
      21. security@vmware.com - VENDOR\_ADVISORY
      22. Vulnerable Software & Versions: (show all)
      23. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.20
      24. ...
    - CVE-2022-22970 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.5)
      8. Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.21
      18. ...
    - CVE-2021-22060 suppress
      1. 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      12. security@vmware.com - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - VENDOR\_ADVISORY
      14. Vulnerable Software & Versions: (show all)
      15. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.18
      16. ...
    - CVE-2021-22096 suppress
      1. In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.
      2. CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2021-22096] CWE-117: Improper Output Neutralization for Logs
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096
      12. OSSIndex - https://tanzu.vmware.com/security/cve-2021-22096
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      16. security@vmware.com - THIRD\_PARTY\_ADVISORY
      17. security@vmware.com - THIRD\_PARTY\_ADVISORY
      18. security@vmware.com - VENDOR\_ADVISORY
      19. Vulnerable Software & Versions: (show all)
      20. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.17
      21. ...
* spring-webmvc-5.2.3.RELEASE.jar
  + Spring Web MVC
    - CVE-2022-22965 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: VMware Spring Framework
      3. Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
      4. Date Added: 2022-04-04
      5. Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
      6. Required Action: Apply updates per vendor instructions.
      7. Due Date: 2022-04-25
      8. Notes: https://nvd.nist.gov/vuln/detail/CVE-2022-22965
      9. 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.
      10. CWE-94 Improper Control of Generation of Code ('Code Injection')
      11. CVSSv3:
      12. Base Score: CRITICAL (9.8)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      14. CVSSv2:
      15. Base Score: HIGH (7.5)
      16. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      17. References:
      18. OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
      19. OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest\_sys/status/1509053689331335174
      20. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
      21. OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
      22. OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
      23. OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
      24. OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/
      25. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      26. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      27. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      28. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      29. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      30. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      31. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      32. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      33. security@vmware.com - EXPLOIT,THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      34. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      35. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      36. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      37. security@vmware.com - THIRD\_PARTY\_ADVISORY
      38. security@vmware.com - THIRD\_PARTY\_ADVISORY
      39. security@vmware.com - THIRD\_PARTY\_ADVISORY
      40. security@vmware.com - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      41. Vulnerable Software & Versions: (show all)
      42. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      43. ...
    - CVE-2024-38816 (OSSINDEX) suppress
      1. Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can craft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running.
      2. Specifically, an application is vulnerable when both of the following are true:
      3. \* the web application uses RouterFunctions to serve static resources
      4. \* resource handling is explicitly configured with a FileSystemResource location
      5. However, malicious requests are blocked and rejected when any of the following is true:
      6. \* the Spring Security HTTP Firewall https://docs.spring.io/spring-security/reference/servlet/exploits/firewall.html is in use
      7. \* the application runs on Tomcat or Jetty
      8. CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
      9. CVSSv2:
      10. Base Score: HIGH (8.199999809265137)
      11. Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
      12. References:
      13. OSSINDEX - [CVE-2024-38816] CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
      14. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38816
      15. OSSIndex - https://spring.io/security/cve-2024-38816
      16. Vulnerable Software & Versions (OSSINDEX):
      17. cpe:2.3:a:org.springframework:spring-webmvc:5.2.3.RELEASE:\*:\*:\*:\*:\*:\*:\*
    - CVE-2021-22118 suppress
      1. In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.
      2. CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.6)
      8. Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      18. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      19. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      20. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      21. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@vmware.com - THIRD\_PARTY\_ADVISORY
      23. security@vmware.com - THIRD\_PARTY\_ADVISORY
      24. Vulnerable Software & Versions: (show all)
      25. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.15
      26. ...
    - CVE-2020-5421 suppress
      1. In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.6)
      8. Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      18. security@pivotal.io - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      19. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      20. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      21. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@pivotal.io - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@pivotal.io - THIRD\_PARTY\_ADVISORY
      25. security@pivotal.io - VENDOR\_ADVISORY
      26. Vulnerable Software & Versions: (show all)
      27. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.9
      28. ...
    - CVE-2022-22950 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      12. Vulnerable Software & Versions: (show all)
      13. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 5.2.20
      14. ...
    - CVE-2022-22971 suppress
      1. 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. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.21
      18. ...
    - CVE-2023-20861 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      8. security@vmware.com - VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.22
      11. ...
    - CVE-2023-20863 suppress
      1. 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.
      2. CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      8. security@vmware.com - VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
      11. ...
    - CVE-2022-22968 suppress
      1. 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.
      2. CWE-178 Improper Handling of Case Sensitivity
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      13. security@vmware.com - THIRD\_PARTY\_ADVISORY
      14. security@vmware.com - THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - VENDOR\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.20
      18. ...
    - CVE-2022-22970 suppress
      1. 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.
      2. CWE-770 Allocation of Resources Without Limits or Throttling
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: LOW (3.5)
      8. Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@vmware.com - MITIGATION,VENDOR\_ADVISORY
      14. security@vmware.com - PATCH,THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions up to (including) 5.2.21
      18. ...
    - CVE-2021-22060 suppress
      1. 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. OSSINDEX - [CVE-2021-22060] CWE-noinfo
      11. OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060
      12. OSSIndex - https://tanzu.vmware.com/security/cve-2021-22060
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      15. security@vmware.com - THIRD\_PARTY\_ADVISORY
      16. security@vmware.com - VENDOR\_ADVISORY
      17. Vulnerable Software & Versions: (show all)
      18. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.18
      19. ...
    - CVE-2021-22096 suppress
      1. In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.
      2. CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      13. security@vmware.com - THIRD\_PARTY\_ADVISORY
      14. security@vmware.com - THIRD\_PARTY\_ADVISORY
      15. security@vmware.com - VENDOR\_ADVISORY
      16. Vulnerable Software & Versions: (show all)
      17. cpe:2.3:a:vmware:spring\_framework:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 5.2.0; versions up to (including) 5.2.17
      18. ...
* tomcat-embed-core-9.0.30.jar
  + Core Tomcat implementation
    - CVE-2020-1938 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: Apache Tomcat
      3. Name: Apache Tomcat Improper Privilege Management Vulnerability
      4. Date Added: 2022-03-03
      5. Description: Apache Tomcat treats Apache JServ Protocol (AJP) connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited.
      6. Required Action: Apply updates per vendor instructions.
      7. Due Date: 2022-03-17
      8. Notes: https://nvd.nist.gov/vuln/detail/CVE-2020-1938
         1. When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, 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. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.
      9. NVD-CWE-Other
      10. CVSSv3:
      11. Base Score: CRITICAL (9.8)
      12. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      13. CVSSv2:
      14. Base Score: HIGH (7.5)
      15. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      16. References:
      17. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,MAILING\_LIST
      18. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      19. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      20. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      21. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      22. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      23. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      24. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      25. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      26. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      27. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      28. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      29. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      30. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      31. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      32. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      33. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      34. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      35. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      36. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      37. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      38. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      39. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      40. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      41. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      42. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      43. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      44. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH
      45. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH
      46. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH
      47. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      48. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      49. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      50. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      51. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      52. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      53. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      54. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      55. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      56. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      57. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      58. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      59. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      60. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      61. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      62. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      63. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      64. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      65. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      66. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      67. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      68. security@apache.org - EXPLOIT,MAILING\_LIST
      69. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      70. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      71. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      72. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      73. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      74. security@apache.org - MAILING\_LIST
      75. security@apache.org - MAILING\_LIST
      76. security@apache.org - MAILING\_LIST
      77. security@apache.org - MAILING\_LIST
      78. security@apache.org - MAILING\_LIST
      79. security@apache.org - MAILING\_LIST
      80. security@apache.org - MAILING\_LIST
      81. security@apache.org - MAILING\_LIST
      82. security@apache.org - MAILING\_LIST
      83. security@apache.org - MAILING\_LIST
      84. security@apache.org - MAILING\_LIST
      85. security@apache.org - MAILING\_LIST
      86. security@apache.org - MAILING\_LIST
      87. security@apache.org - MAILING\_LIST
      88. security@apache.org - MAILING\_LIST
      89. security@apache.org - MAILING\_LIST
      90. security@apache.org - MAILING\_LIST
      91. security@apache.org - MAILING\_LIST
      92. security@apache.org - MAILING\_LIST
      93. security@apache.org - MAILING\_LIST
      94. security@apache.org - MAILING\_LIST
      95. security@apache.org - MAILING\_LIST,PATCH
      96. security@apache.org - MAILING\_LIST,PATCH
      97. security@apache.org - MAILING\_LIST,PATCH
      98. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      99. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      100. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      101. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      102. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      103. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      104. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      105. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      106. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      107. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      108. security@apache.org - RELEASE\_NOTES
      109. security@apache.org - RELEASE\_NOTES
      110. security@apache.org - RELEASE\_NOTES
      111. security@apache.org - THIRD\_PARTY\_ADVISORY
      112. security@apache.org - THIRD\_PARTY\_ADVISORY
      113. security@apache.org - THIRD\_PARTY\_ADVISORY
      114. security@apache.org - THIRD\_PARTY\_ADVISORY
      115. security@apache.org - THIRD\_PARTY\_ADVISORY
      116. security@apache.org - THIRD\_PARTY\_ADVISORY
      117. security@apache.org - THIRD\_PARTY\_ADVISORY
      118. security@apache.org - THIRD\_PARTY\_ADVISORY
      119. Vulnerable Software & Versions: (show all)
      120. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.31
      121. ...
    - CVE-2025-24813 suppress
      1. Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.
      2. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98.
      3. If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:
      4. - writes enabled for the default servlet (disabled by default)
      5. - support for partial PUT (enabled by default)
      6. - a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads
      7. - attacker knowledge of the names of security sensitive files being uploaded
      8. - the security sensitive files also being uploaded via partial PUT
      9. If all of the following were true, a malicious user was able to perform remote code execution:
      10. - writes enabled for the default servlet (disabled by default)
      11. - support for partial PUT (enabled by default)
      12. - application was using Tomcat's file based session persistence with the default storage location
      13. - application included a library that may be leveraged in a deserialization attack
      14. Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.
      15. CWE-44 Path Equivalence: 'file.name' (Internal Dot), CWE-502 Deserialization of Untrusted Data, CWE-706 Use of Incorrectly-Resolved Name or Reference
      16. CVSSv3:
      17. Base Score: CRITICAL (9.8)
      18. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      19. References:
      20. 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT
      21. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - VENDOR\_ADVISORY
      23. Vulnerable Software & Versions: (show all)
      24. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.99
      25. ...
    - CVE-2020-11996 suppress
      1. 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      23. security@apache.org - THIRD\_PARTY\_ADVISORY
      24. security@apache.org - THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.35
      30. ...
    - CVE-2020-13934 suppress
      1. An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.
      2. CWE-401 Missing Release of Memory after Effective Lifetime, CWE-476 NULL Pointer Dereference
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      23. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      26. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      27. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      28. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      29. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      30. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      31. security@apache.org - THIRD\_PARTY\_ADVISORY
      32. security@apache.org - THIRD\_PARTY\_ADVISORY
      33. security@apache.org - THIRD\_PARTY\_ADVISORY
      34. Vulnerable Software & Versions: (show all)
      35. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.36
      36. ...
    - CVE-2020-13935 suppress
      1. The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.
      2. CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      25. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      27. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      28. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      29. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      30. security@apache.org - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      31. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      32. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      33. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      34. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      35. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      36. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      37. security@apache.org - THIRD\_PARTY\_ADVISORY
      38. security@apache.org - THIRD\_PARTY\_ADVISORY
      39. security@apache.org - THIRD\_PARTY\_ADVISORY
      40. security@apache.org - THIRD\_PARTY\_ADVISORY
      41. security@apache.org - THIRD\_PARTY\_ADVISORY
      42. Vulnerable Software & Versions: (show all)
      43. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.36
      44. ...
    - CVE-2020-17527 suppress
      1. While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 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. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.
      2. CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. Vulnerable Software & Versions: (show all)
      31. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.35
      32. ...
    - CVE-2021-25122 suppress
      1. When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.
      2. CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.41
      30. ...
    - CVE-2021-41079 suppress
      1. Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.
      2. CWE-20 Improper Input Validation, CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      16. security@apache.org - THIRD\_PARTY\_ADVISORY
      17. security@apache.org - THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions: (show all)
      19. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.44
      20. ...
    - CVE-2022-29885 suppress
      1. The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.
      2. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,MITIGATION,VENDOR\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.13; versions up to (including) 9.0.62
      22. ...
    - CVE-2022-42252 suppress
      1. If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      8. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.68
      11. ...
    - CVE-2023-44487 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: IETF HTTP/2
      3. Name: HTTP/2 Rapid Reset Attack Vulnerability
      4. Date Added: 2023-10-10
      5. Description: HTTP/2 contains a rapid reset vulnerability that allows for a distributed denial-of-service attack (DDoS).
      6. Required Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
      7. Due Date: 2023-10-31
      8. Notes: This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/ ; https://nvd.nist.gov/vuln/detail/CVE-2023-44487
      9. The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.
      10. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      11. CVSSv3:
      12. Base Score: HIGH (7.5)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      14. References:
      15. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      18. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      19. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      20. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      21. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      22. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      23. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      24. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      25. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      26. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      27. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      28. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      29. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      30. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      31. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      32. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      33. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      34. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      35. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      36. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      37. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MITIGATION,VENDOR\_ADVISORY
      38. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      39. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      40. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      41. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      42. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      43. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      44. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      45. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      46. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      47. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      48. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      49. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      50. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      51. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PRESS/MEDIA\_COVERAGE
      52. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      53. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,VENDOR\_ADVISORY
      54. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,VENDOR\_ADVISORY
      55. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,VENDOR\_ADVISORY
      56. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      57. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      58. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      59. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      60. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      61. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      62. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      63. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      64. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      65. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      66. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      67. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      68. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      69. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      70. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      71. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      72. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      73. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      74. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      75. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      76. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      77. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      78. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      79. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      80. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      81. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      82. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      83. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      84. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      85. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      86. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      87. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      88. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      89. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      90. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      91. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      92. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      93. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      94. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      95. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      96. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      97. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      98. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      99. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      100. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      101. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,PATCH,VENDOR\_ADVISORY
      102. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,PATCH,VENDOR\_ADVISORY
      103. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      104. af854a3a-2127-422b-91ae-364da2661108 - PATCH
      105. af854a3a-2127-422b-91ae-364da2661108 - PATCH
      106. af854a3a-2127-422b-91ae-364da2661108 - PATCH
      107. af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR\_ADVISORY
      108. af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR\_ADVISORY
      109. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE
      110. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      111. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      112. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      113. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      114. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT
      115. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT
      116. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT,RELEASE\_NOTES
      117. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT,THIRD\_PARTY\_ADVISORY
      118. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      119. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      120. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      121. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,VENDOR\_ADVISORY
      122. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,THIRD\_PARTY\_ADVISORY
      123. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      124. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      125. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      126. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      127. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      128. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      129. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      130. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      131. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      132. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      133. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      134. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      135. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      136. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      137. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      138. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      139. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      140. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      141. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      142. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      143. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      144. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      145. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      146. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      147. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      148. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      149. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      150. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      151. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      152. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      153. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      154. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      155. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      156. cve@mitre.org - EXPLOIT,THIRD\_PARTY\_ADVISORY
      157. cve@mitre.org - EXPLOIT,THIRD\_PARTY\_ADVISORY
      158. cve@mitre.org - ISSUE\_TRACKING
      159. cve@mitre.org - ISSUE\_TRACKING
      160. cve@mitre.org - ISSUE\_TRACKING
      161. cve@mitre.org - ISSUE\_TRACKING
      162. cve@mitre.org - ISSUE\_TRACKING
      163. cve@mitre.org - ISSUE\_TRACKING
      164. cve@mitre.org - ISSUE\_TRACKING
      165. cve@mitre.org - ISSUE\_TRACKING
      166. cve@mitre.org - ISSUE\_TRACKING
      167. cve@mitre.org - ISSUE\_TRACKING
      168. cve@mitre.org - ISSUE\_TRACKING
      169. cve@mitre.org - ISSUE\_TRACKING
      170. cve@mitre.org - ISSUE\_TRACKING
      171. cve@mitre.org - ISSUE\_TRACKING
      172. cve@mitre.org - ISSUE\_TRACKING
      173. cve@mitre.org - ISSUE\_TRACKING
      174. cve@mitre.org - ISSUE\_TRACKING
      175. cve@mitre.org - ISSUE\_TRACKING
      176. cve@mitre.org - ISSUE\_TRACKING
      177. cve@mitre.org - ISSUE\_TRACKING
      178. cve@mitre.org - ISSUE\_TRACKING,MITIGATION,VENDOR\_ADVISORY
      179. cve@mitre.org - ISSUE\_TRACKING,PATCH
      180. cve@mitre.org - ISSUE\_TRACKING,PATCH
      181. cve@mitre.org - ISSUE\_TRACKING,PATCH
      182. cve@mitre.org - ISSUE\_TRACKING,PATCH
      183. cve@mitre.org - ISSUE\_TRACKING,PATCH
      184. cve@mitre.org - ISSUE\_TRACKING,PATCH
      185. cve@mitre.org - ISSUE\_TRACKING,PATCH
      186. cve@mitre.org - ISSUE\_TRACKING,PATCH
      187. cve@mitre.org - ISSUE\_TRACKING,PATCH
      188. cve@mitre.org - ISSUE\_TRACKING,PATCH
      189. cve@mitre.org - ISSUE\_TRACKING,PATCH
      190. cve@mitre.org - ISSUE\_TRACKING,PATCH
      191. cve@mitre.org - ISSUE\_TRACKING,PATCH
      192. cve@mitre.org - ISSUE\_TRACKING,PRESS/MEDIA\_COVERAGE
      193. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      194. cve@mitre.org - ISSUE\_TRACKING,VENDOR\_ADVISORY
      195. cve@mitre.org - ISSUE\_TRACKING,VENDOR\_ADVISORY
      196. cve@mitre.org - ISSUE\_TRACKING,VENDOR\_ADVISORY
      197. cve@mitre.org - MAILING\_LIST
      198. cve@mitre.org - MAILING\_LIST
      199. cve@mitre.org - MAILING\_LIST
      200. cve@mitre.org - MAILING\_LIST
      201. cve@mitre.org - MAILING\_LIST
      202. cve@mitre.org - MAILING\_LIST
      203. cve@mitre.org - MAILING\_LIST
      204. cve@mitre.org - MAILING\_LIST
      205. cve@mitre.org - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      206. cve@mitre.org - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      207. cve@mitre.org - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      208. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      209. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      210. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      211. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      212. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      213. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      214. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      215. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      216. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      217. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      218. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      219. cve@mitre.org - MAILING\_LIST,VENDOR\_ADVISORY
      220. cve@mitre.org - MAILING\_LIST,VENDOR\_ADVISORY
      221. cve@mitre.org - MITIGATION,PATCH,VENDOR\_ADVISORY
      222. cve@mitre.org - MITIGATION,PATCH,VENDOR\_ADVISORY
      223. cve@mitre.org - MITIGATION,VENDOR\_ADVISORY
      224. cve@mitre.org - PATCH
      225. cve@mitre.org - PATCH
      226. cve@mitre.org - PATCH
      227. cve@mitre.org - PATCH,VENDOR\_ADVISORY
      228. cve@mitre.org - PATCH,VENDOR\_ADVISORY
      229. cve@mitre.org - PRESS/MEDIA\_COVERAGE
      230. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      231. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      232. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      233. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      234. cve@mitre.org - PRODUCT
      235. cve@mitre.org - PRODUCT
      236. cve@mitre.org - PRODUCT,RELEASE\_NOTES
      237. cve@mitre.org - PRODUCT,THIRD\_PARTY\_ADVISORY
      238. cve@mitre.org - RELEASE\_NOTES
      239. cve@mitre.org - RELEASE\_NOTES
      240. cve@mitre.org - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      241. cve@mitre.org - RELEASE\_NOTES,VENDOR\_ADVISORY
      242. cve@mitre.org - TECHNICAL\_DESCRIPTION,THIRD\_PARTY\_ADVISORY
      243. cve@mitre.org - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      244. cve@mitre.org - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      245. cve@mitre.org - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      246. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      247. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      248. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      249. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      250. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      251. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      252. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      253. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      254. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      255. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      256. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      257. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      258. cve@mitre.org - THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      259. cve@mitre.org - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      260. cve@mitre.org - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      261. cve@mitre.org - VENDOR\_ADVISORY
      262. cve@mitre.org - VENDOR\_ADVISORY
      263. cve@mitre.org - VENDOR\_ADVISORY
      264. cve@mitre.org - VENDOR\_ADVISORY
      265. cve@mitre.org - VENDOR\_ADVISORY
      266. cve@mitre.org - VENDOR\_ADVISORY
      267. cve@mitre.org - VENDOR\_ADVISORY
      268. cve@mitre.org - VENDOR\_ADVISORY
      269. cve@mitre.org - VENDOR\_ADVISORY
      270. cve@mitre.org - VENDOR\_ADVISORY
      271. cve@mitre.org - VENDOR\_ADVISORY
      272. cve@mitre.org - VENDOR\_ADVISORY
      273. cve@mitre.org - VENDOR\_ADVISORY
      274. cve@mitre.org - VENDOR\_ADVISORY
      275. Vulnerable Software & Versions: (show all)
      276. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.80
      277. ...
    - CVE-2023-46589 suppress
      1. Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 through 9.0.82 and from 8.5.0 through 8.5.95 did not correctly parse HTTP trailer headers. A trailer header that exceeded the header size limit could cause Tomcat to treat a single
      2. request as multiple requests leading to the possibility of request
      3. smuggling when behind a reverse proxy.
      4. Users are recommended to upgrade to version 11.0.0-M11 onwards, 10.1.16 onwards, 9.0.83 onwards or 8.5.96 onwards, which fix the issue.
      5. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      6. CVSSv3:
      7. Base Score: HIGH (7.5)
      8. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      14. Vulnerable Software & Versions: (show all)
      15. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.83
      16. ...
    - CVE-2024-38286 suppress
      1. Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.
      2. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89. Older, unsupported versions may also be affected.
      3. Users are recommended to upgrade to version 11.0.0-M21, 10.1.25, or 9.0.90, which fixes the issue.
      4. Apache Tomcat, under certain configurations on any platform, allows an attacker to cause an OutOfMemoryError by abusing the TLS handshake process.
      5. CWE-770 Allocation of Resources Without Limits or Throttling
      6. CVSSv3:
      7. Base Score: HIGH (7.5)
      8. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. security@apache.org - MAILING\_LIST
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.13; versions up to (excluding) 9.0.90
      15. ...
    - CVE-2020-9484 suppress
      1. When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) 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; and d) 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. Note that all of conditions a) to d) must be true for the attack to succeed.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: HIGH (7.0)
      5. Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.4)
      8. Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,MITIGATION,PATCH,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      25. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      26. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      27. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      28. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      29. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      30. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      31. security@apache.org - MAILING\_LIST,MITIGATION,PATCH,THIRD\_PARTY\_ADVISORY
      32. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      33. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      34. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      35. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      36. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      37. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      38. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      39. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      40. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      41. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      42. security@apache.org - THIRD\_PARTY\_ADVISORY
      43. security@apache.org - THIRD\_PARTY\_ADVISORY
      44. security@apache.org - THIRD\_PARTY\_ADVISORY
      45. security@apache.org - THIRD\_PARTY\_ADVISORY
      46. security@apache.org - THIRD\_PARTY\_ADVISORY
      47. security@apache.org - THIRD\_PARTY\_ADVISORY
      48. security@apache.org - THIRD\_PARTY\_ADVISORY
      49. security@apache.org - THIRD\_PARTY\_ADVISORY
      50. security@apache.org - THIRD\_PARTY\_ADVISORY
      51. security@apache.org - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      52. Vulnerable Software & Versions: (show all)
      53. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.43
      54. ...
    - CVE-2021-25329 suppress
      1. The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: HIGH (7.0)
      5. Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.4)
      8. Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.41
      30. ...
    - CVE-2021-30640 suppress
      1. 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. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.
      2. CWE-116 Improper Encoding or Escaping of Output
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      21. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - THIRD\_PARTY\_ADVISORY
      24. security@apache.org - THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.46
      30. ...
    - CVE-2022-34305 suppress
      1. In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.
      2. CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
      3. CVSSv3:
      4. Base Score: MEDIUM (6.1)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. security@apache.org - MAILING\_LIST,RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. security@apache.org - THIRD\_PARTY\_ADVISORY
      17. security@apache.org - THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions: (show all)
      19. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.30; versions up to (including) 9.0.64
      20. ...
      21. CVE-2023-41080 suppress
      22. URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92.
      23. The vulnerability is limited to the ROOT (default) web application.
      24. CWE-601 URL Redirection to Untrusted Site ('Open Redirect')
      25. CVSSv3:
      26. Base Score: MEDIUM (6.1)
      27. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A
      28. References:
      29. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH,VENDOR\_ADVISORY
      30. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      31. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      32. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      33. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      34. security@apache.org - ISSUE\_TRACKING,PATCH,VENDOR\_ADVISORY
      35. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      36. security@apache.org - THIRD\_PARTY\_ADVISORY
      37. security@apache.org - THIRD\_PARTY\_ADVISORY
      38. security@apache.org - THIRD\_PARTY\_ADVISORY
      39. Vulnerable Software & Versions: (show all)
      40. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.79
      41. ...
    - CVE-2021-24122 suppress
      1. When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.
      2. CWE-706 Use of Incorrectly-Resolved Name or Reference, CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: MEDIUM (5.9)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.39
      22. ...
    - CVE-2021-33037 suppress
      1. Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 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. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. Vulnerable Software & Versions: (show all)
      31. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (excluding) 9.0.0; versions up to (including) 9.0.46
      32. ...
    - CVE-2023-42795 suppress
      1. Incomplete Cleanup vulnerability in Apache Tomcat.When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an error could
      2. cause Tomcat to skip some parts of the recycling process leading to
      3. information leaking from the current request/response to the next.
      4. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.
      5. CWE-459 Incomplete Cleanup
      6. CVSSv3:
      7. Base Score: MEDIUM (5.3)
      8. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.81
      22. ...
    - CVE-2023-45648 suppress
      1. Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially
      2. crafted, invalid trailer header could cause Tomcat to treat a single
      3. request as multiple requests leading to the possibility of request
      4. smuggling when behind a reverse proxy.
      5. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.
      6. CWE-20 Improper Input Validation, NVD-CWE-Other
      7. CVSSv3:
      8. Base Score: MEDIUM (5.3)
      9. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      10. References:
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - VENDOR\_ADVISORY
      21. Vulnerable Software & Versions: (show all)
      22. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.81
      23. ...
    - CVE-2024-21733 suppress
      1. Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43.
      2. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.
      3. CWE-209 Generation of Error Message Containing Sensitive Information
      4. CVSSv3:
      5. Base Score: MEDIUM (5.3)
      6. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A
      7. References:
      8. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      9. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      10. security@apache.org - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      11. security@apache.org - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      12. Vulnerable Software & Versions: (show all)
      13. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.44
      14. ...
    - CVE-2019-17569 suppress
      1. 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.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: MEDIUM (4.8)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.28; versions up to (including) 9.0.30
      30. ...
    - CVE-2020-1935 suppress
      1. In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led 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.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: MEDIUM (4.8)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - BROKEN\_LINK,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. security@apache.org - BROKEN\_LINK,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. security@apache.org - THIRD\_PARTY\_ADVISORY
      31. security@apache.org - THIRD\_PARTY\_ADVISORY
      32. Vulnerable Software & Versions: (show all)
      33. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.30
      34. ...
    - CVE-2020-13943 suppress
      1. If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 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. This could lead to users seeing responses for unexpected resources.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - BROKEN\_LINK
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      17. security@apache.org - BROKEN\_LINK
      18. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      19. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - THIRD\_PARTY\_ADVISORY
      21. security@apache.org - THIRD\_PARTY\_ADVISORY
      22. security@apache.org - THIRD\_PARTY\_ADVISORY
      23. security@apache.org - VENDOR\_ADVISORY
      24. Vulnerable Software & Versions: (show all)
      25. cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*
      26. ...
    - CVE-2023-28708 suppress
      1. When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.
      2. CWE-523 Unprotected Transport of Credentials
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      8. security@apache.org - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (excluding) 9.0.0; versions up to (excluding) 9.0.72
      11. ...
    - CVE-2021-43980 suppress
      1. The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client.
      2. CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
      3. CVSSv3:
      4. Base Score: LOW (3.7)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:2.2/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      8. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      9. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      14. security@apache.org - THIRD\_PARTY\_ADVISORY
      15. Vulnerable Software & Versions: (show all)
      16. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.60
      17. ...
* tomcat-embed-websocket-9.0.30.jar
  + Core Tomcat implementation
    - CVE-2020-1938 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: Apache Tomcat
      3. Name: Apache Tomcat Improper Privilege Management Vulnerability
      4. Date Added: 2022-03-03
      5. Description: Apache Tomcat treats Apache JServ Protocol (AJP) connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited.
      6. Required Action: Apply updates per vendor instructions.
      7. Due Date: 2022-03-17
      8. Notes: https://nvd.nist.gov/vuln/detail/CVE-2020-1938
      9. When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, 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. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.
      10. NVD-CWE-Other
      11. CVSSv3:
      12. Base Score: CRITICAL (9.8)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      14. CVSSv2:
      15. Base Score: HIGH (7.5)
      16. Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P
      17. References:
      18. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,MAILING\_LIST
      19. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      20. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      21. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      22. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      23. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MAILING\_LIST
      24. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      25. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      26. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      27. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      28. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      29. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      30. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      31. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      32. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      33. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      34. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      35. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      36. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      37. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      38. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      39. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      40. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      41. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      42. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      43. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      44. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      45. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH
      46. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH
      47. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH
      48. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      49. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      50. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      51. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      52. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      53. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      54. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      55. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      56. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      57. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      58. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      59. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      60. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      61. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      62. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      63. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      64. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      65. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      66. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      67. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      68. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      69. security@apache.org - EXPLOIT,MAILING\_LIST
      70. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      71. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      72. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      73. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      74. security@apache.org - ISSUE\_TRACKING,MAILING\_LIST
      75. security@apache.org - MAILING\_LIST
      76. security@apache.org - MAILING\_LIST
      77. security@apache.org - MAILING\_LIST
      78. security@apache.org - MAILING\_LIST
      79. security@apache.org - MAILING\_LIST
      80. security@apache.org - MAILING\_LIST
      81. security@apache.org - MAILING\_LIST
      82. security@apache.org - MAILING\_LIST
      83. security@apache.org - MAILING\_LIST
      84. security@apache.org - MAILING\_LIST
      85. security@apache.org - MAILING\_LIST
      86. security@apache.org - MAILING\_LIST
      87. security@apache.org - MAILING\_LIST
      88. security@apache.org - MAILING\_LIST
      89. security@apache.org - MAILING\_LIST
      90. security@apache.org - MAILING\_LIST
      91. security@apache.org - MAILING\_LIST
      92. security@apache.org - MAILING\_LIST
      93. security@apache.org - MAILING\_LIST
      94. security@apache.org - MAILING\_LIST
      95. security@apache.org - MAILING\_LIST
      96. security@apache.org - MAILING\_LIST,PATCH
      97. security@apache.org - MAILING\_LIST,PATCH
      98. security@apache.org - MAILING\_LIST,PATCH
      99. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      100. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      101. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      102. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      103. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      104. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      105. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      106. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      107. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      108. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      109. security@apache.org - RELEASE\_NOTES
      110. security@apache.org - RELEASE\_NOTES
      111. security@apache.org - RELEASE\_NOTES
      112. security@apache.org - THIRD\_PARTY\_ADVISORY
      113. security@apache.org - THIRD\_PARTY\_ADVISORY
      114. security@apache.org - THIRD\_PARTY\_ADVISORY
      115. security@apache.org - THIRD\_PARTY\_ADVISORY
      116. security@apache.org - THIRD\_PARTY\_ADVISORY
      117. security@apache.org - THIRD\_PARTY\_ADVISORY
      118. security@apache.org - THIRD\_PARTY\_ADVISORY
      119. security@apache.org - THIRD\_PARTY\_ADVISORY
      120. Vulnerable Software & Versions: (show all)
      121. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.31
      122. ...
    - CVE-2025-24813 suppress
      1. Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.
      2. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98.
      3. If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:
      4. - writes enabled for the default servlet (disabled by default)
      5. - support for partial PUT (enabled by default)
      6. - a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads
      7. - attacker knowledge of the names of security sensitive files being uploaded
      8. - the security sensitive files also being uploaded via partial PUT
      9. If all of the following were true, a malicious user was able to perform remote code execution:
      10. - writes enabled for the default servlet (disabled by default)
      11. - support for partial PUT (enabled by default)
      12. - application was using Tomcat's file based session persistence with the default storage location
      13. - application included a library that may be leveraged in a deserialization attack
      14. Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.
      15. CWE-44 Path Equivalence: 'file.name' (Internal Dot), CWE-502 Deserialization of Untrusted Data, CWE-706 Use of Incorrectly-Resolved Name or Reference
      16. CVSSv3:
      17. Base Score: CRITICAL (9.8)
      18. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A
      19. References:
      20. 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT
      21. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - VENDOR\_ADVISORY
      23. Vulnerable Software & Versions: (show all)
      24. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.99
      25. ...
    - CVE-2020-8022 suppress
      1. A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.
      2. CWE-276 Incorrect Default Permissions
      3. CVSSv3:
      4. Base Score: HIGH (7.8)
      5. Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: HIGH (7.2)
      8. Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,ISSUE\_TRACKING,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. meissner@suse.de - EXPLOIT,ISSUE\_TRACKING,VENDOR\_ADVISORY
      13. meissner@suse.de - MAILING\_LIST,VENDOR\_ADVISORY
      14. Vulnerable Software & Versions: (show all)
      15. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions up to (excluding) 9.0.35-3.39.1
      16. ...
    - CVE-2020-11996 suppress
      1. 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.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      23. security@apache.org - THIRD\_PARTY\_ADVISORY
      24. security@apache.org - THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.35
      30. ...
    - CVE-2020-13934 suppress
      1. An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.
      2. CWE-401 Missing Release of Memory after Effective Lifetime, CWE-476 NULL Pointer Dereference
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      23. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      26. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      27. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      28. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      29. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      30. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      31. security@apache.org - THIRD\_PARTY\_ADVISORY
      32. security@apache.org - THIRD\_PARTY\_ADVISORY
      33. security@apache.org - THIRD\_PARTY\_ADVISORY
      34. Vulnerable Software & Versions: (show all)
      35. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.36
      36. ...
    - CVE-2020-13935 suppress
      1. The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.
      2. CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      25. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      27. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      28. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      29. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      30. security@apache.org - NOT\_APPLICABLE,THIRD\_PARTY\_ADVISORY
      31. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      32. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      33. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      34. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      35. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      36. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      37. security@apache.org - THIRD\_PARTY\_ADVISORY
      38. security@apache.org - THIRD\_PARTY\_ADVISORY
      39. security@apache.org - THIRD\_PARTY\_ADVISORY
      40. security@apache.org - THIRD\_PARTY\_ADVISORY
      41. security@apache.org - THIRD\_PARTY\_ADVISORY
      42. Vulnerable Software & Versions: (show all)
      43. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.36
      44. ...
    - CVE-2020-17527 suppress
      1. While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 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. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.
      2. CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. Vulnerable Software & Versions: (show all)
      31. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.35
      32. ...
    - CVE-2021-25122 suppress
      1. When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.
      2. CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.41
      30. ...
    - CVE-2021-41079 suppress
      1. Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.
      2. CWE-20 Improper Input Validation, CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      16. security@apache.org - THIRD\_PARTY\_ADVISORY
      17. security@apache.org - THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions: (show all)
      19. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.44
      20. ...
    - CVE-2022-29885 suppress
      1. The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.
      2. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,MITIGATION,VENDOR\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,MITIGATION,VENDOR\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.13; versions up to (including) 9.0.62
      22. ...
    - CVE-2022-42252 suppress
      1. If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: HIGH (7.5)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      8. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.68
      11. ...
    - CVE-2023-44487 suppress
      1. CISA Known Exploited Vulnerability:
      2. Product: IETF HTTP/2
      3. Name: HTTP/2 Rapid Reset Attack Vulnerability
      4. Date Added: 2023-10-10
      5. Description: HTTP/2 contains a rapid reset vulnerability that allows for a distributed denial-of-service attack (DDoS).
      6. Required Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
      7. Due Date: 2023-10-31
      8. Notes: This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/ ; https://nvd.nist.gov/vuln/detail/CVE-2023-44487
      9. The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.
      10. CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo
      11. CVSSv3:
      12. Base Score: HIGH (7.5)
      13. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      14. References:
      15. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      18. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      19. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      20. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      21. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      22. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      23. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      24. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      25. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      26. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      27. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      28. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      29. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      30. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      31. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      32. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      33. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      34. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      35. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      36. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING
      37. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,MITIGATION,VENDOR\_ADVISORY
      38. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      39. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      40. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      41. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      42. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      43. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      44. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      45. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      46. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      47. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      48. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      49. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      50. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH
      51. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PRESS/MEDIA\_COVERAGE
      52. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      53. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,VENDOR\_ADVISORY
      54. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,VENDOR\_ADVISORY
      55. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,VENDOR\_ADVISORY
      56. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      57. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      58. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      59. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      60. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      61. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      62. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      63. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      64. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      65. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      66. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      67. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      68. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      69. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      70. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      71. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      72. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      73. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      74. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      75. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      76. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      77. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      78. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      79. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      80. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      81. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      82. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      83. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      84. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      85. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      86. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      87. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      88. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      89. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      90. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      91. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      92. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      93. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      94. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      95. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      96. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      97. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      98. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      99. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      100. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      101. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,PATCH,VENDOR\_ADVISORY
      102. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,PATCH,VENDOR\_ADVISORY
      103. af854a3a-2127-422b-91ae-364da2661108 - MITIGATION,VENDOR\_ADVISORY
      104. af854a3a-2127-422b-91ae-364da2661108 - PATCH
      105. af854a3a-2127-422b-91ae-364da2661108 - PATCH
      106. af854a3a-2127-422b-91ae-364da2661108 - PATCH
      107. af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR\_ADVISORY
      108. af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR\_ADVISORY
      109. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE
      110. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      111. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      112. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      113. af854a3a-2127-422b-91ae-364da2661108 - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      114. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT
      115. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT
      116. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT,RELEASE\_NOTES
      117. af854a3a-2127-422b-91ae-364da2661108 - PRODUCT,THIRD\_PARTY\_ADVISORY
      118. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      119. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES
      120. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      121. af854a3a-2127-422b-91ae-364da2661108 - RELEASE\_NOTES,VENDOR\_ADVISORY
      122. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,THIRD\_PARTY\_ADVISORY
      123. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      124. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      125. af854a3a-2127-422b-91ae-364da2661108 - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      126. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      127. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      128. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      129. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      130. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      131. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      132. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      133. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      134. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      135. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      136. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      137. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      138. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      139. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      140. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      141. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      142. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      143. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      144. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      145. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      146. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      147. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      148. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      149. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      150. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      151. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      152. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      153. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      154. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      155. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      156. cve@mitre.org - EXPLOIT,THIRD\_PARTY\_ADVISORY
      157. cve@mitre.org - EXPLOIT,THIRD\_PARTY\_ADVISORY
      158. cve@mitre.org - ISSUE\_TRACKING
      159. cve@mitre.org - ISSUE\_TRACKING
      160. cve@mitre.org - ISSUE\_TRACKING
      161. cve@mitre.org - ISSUE\_TRACKING
      162. cve@mitre.org - ISSUE\_TRACKING
      163. cve@mitre.org - ISSUE\_TRACKING
      164. cve@mitre.org - ISSUE\_TRACKING
      165. cve@mitre.org - ISSUE\_TRACKING
      166. cve@mitre.org - ISSUE\_TRACKING
      167. cve@mitre.org - ISSUE\_TRACKING
      168. cve@mitre.org - ISSUE\_TRACKING
      169. cve@mitre.org - ISSUE\_TRACKING
      170. cve@mitre.org - ISSUE\_TRACKING
      171. cve@mitre.org - ISSUE\_TRACKING
      172. cve@mitre.org - ISSUE\_TRACKING
      173. cve@mitre.org - ISSUE\_TRACKING
      174. cve@mitre.org - ISSUE\_TRACKING
      175. cve@mitre.org - ISSUE\_TRACKING
      176. cve@mitre.org - ISSUE\_TRACKING
      177. cve@mitre.org - ISSUE\_TRACKING
      178. cve@mitre.org - ISSUE\_TRACKING,MITIGATION,VENDOR\_ADVISORY
      179. cve@mitre.org - ISSUE\_TRACKING,PATCH
      180. cve@mitre.org - ISSUE\_TRACKING,PATCH
      181. cve@mitre.org - ISSUE\_TRACKING,PATCH
      182. cve@mitre.org - ISSUE\_TRACKING,PATCH
      183. cve@mitre.org - ISSUE\_TRACKING,PATCH
      184. cve@mitre.org - ISSUE\_TRACKING,PATCH
      185. cve@mitre.org - ISSUE\_TRACKING,PATCH
      186. cve@mitre.org - ISSUE\_TRACKING,PATCH
      187. cve@mitre.org - ISSUE\_TRACKING,PATCH
      188. cve@mitre.org - ISSUE\_TRACKING,PATCH
      189. cve@mitre.org - ISSUE\_TRACKING,PATCH
      190. cve@mitre.org - ISSUE\_TRACKING,PATCH
      191. cve@mitre.org - ISSUE\_TRACKING,PATCH
      192. cve@mitre.org - ISSUE\_TRACKING,PRESS/MEDIA\_COVERAGE
      193. cve@mitre.org - ISSUE\_TRACKING,THIRD\_PARTY\_ADVISORY
      194. cve@mitre.org - ISSUE\_TRACKING,VENDOR\_ADVISORY
      195. cve@mitre.org - ISSUE\_TRACKING,VENDOR\_ADVISORY
      196. cve@mitre.org - ISSUE\_TRACKING,VENDOR\_ADVISORY
      197. cve@mitre.org - MAILING\_LIST
      198. cve@mitre.org - MAILING\_LIST
      199. cve@mitre.org - MAILING\_LIST
      200. cve@mitre.org - MAILING\_LIST
      201. cve@mitre.org - MAILING\_LIST
      202. cve@mitre.org - MAILING\_LIST
      203. cve@mitre.org - MAILING\_LIST
      204. cve@mitre.org - MAILING\_LIST
      205. cve@mitre.org - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      206. cve@mitre.org - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      207. cve@mitre.org - MAILING\_LIST,RELEASE\_NOTES,VENDOR\_ADVISORY
      208. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      209. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      210. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      211. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      212. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      213. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      214. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      215. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      216. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      217. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      218. cve@mitre.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      219. cve@mitre.org - MAILING\_LIST,VENDOR\_ADVISORY
      220. cve@mitre.org - MAILING\_LIST,VENDOR\_ADVISORY
      221. cve@mitre.org - MITIGATION,PATCH,VENDOR\_ADVISORY
      222. cve@mitre.org - MITIGATION,PATCH,VENDOR\_ADVISORY
      223. cve@mitre.org - MITIGATION,VENDOR\_ADVISORY
      224. cve@mitre.org - PATCH
      225. cve@mitre.org - PATCH
      226. cve@mitre.org - PATCH
      227. cve@mitre.org - PATCH,VENDOR\_ADVISORY
      228. cve@mitre.org - PATCH,VENDOR\_ADVISORY
      229. cve@mitre.org - PRESS/MEDIA\_COVERAGE
      230. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      231. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      232. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      233. cve@mitre.org - PRESS/MEDIA\_COVERAGE,THIRD\_PARTY\_ADVISORY
      234. cve@mitre.org - PRODUCT
      235. cve@mitre.org - PRODUCT
      236. cve@mitre.org - PRODUCT,RELEASE\_NOTES
      237. cve@mitre.org - PRODUCT,THIRD\_PARTY\_ADVISORY
      238. cve@mitre.org - RELEASE\_NOTES
      239. cve@mitre.org - RELEASE\_NOTES
      240. cve@mitre.org - RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      241. cve@mitre.org - RELEASE\_NOTES,VENDOR\_ADVISORY
      242. cve@mitre.org - TECHNICAL\_DESCRIPTION,THIRD\_PARTY\_ADVISORY
      243. cve@mitre.org - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      244. cve@mitre.org - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      245. cve@mitre.org - TECHNICAL\_DESCRIPTION,VENDOR\_ADVISORY
      246. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      247. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      248. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      249. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      250. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      251. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      252. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      253. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      254. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      255. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      256. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      257. cve@mitre.org - THIRD\_PARTY\_ADVISORY
      258. cve@mitre.org - THIRD\_PARTY\_ADVISORY,US\_GOVERNMENT\_RESOURCE
      259. cve@mitre.org - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      260. cve@mitre.org - THIRD\_PARTY\_ADVISORY,VENDOR\_ADVISORY
      261. cve@mitre.org - VENDOR\_ADVISORY
      262. cve@mitre.org - VENDOR\_ADVISORY
      263. cve@mitre.org - VENDOR\_ADVISORY
      264. cve@mitre.org - VENDOR\_ADVISORY
      265. cve@mitre.org - VENDOR\_ADVISORY
      266. cve@mitre.org - VENDOR\_ADVISORY
      267. cve@mitre.org - VENDOR\_ADVISORY
      268. cve@mitre.org - VENDOR\_ADVISORY
      269. cve@mitre.org - VENDOR\_ADVISORY
      270. cve@mitre.org - VENDOR\_ADVISORY
      271. cve@mitre.org - VENDOR\_ADVISORY
      272. cve@mitre.org - VENDOR\_ADVISORY
      273. cve@mitre.org - VENDOR\_ADVISORY
      274. cve@mitre.org - VENDOR\_ADVISORY
      275. Vulnerable Software & Versions: (show all)
      276. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.80
      277. ...
    - CVE-2023-46589 suppress
      1. Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 through 9.0.82 and from 8.5.0 through 8.5.95 did not correctly parse HTTP trailer headers. A trailer header that exceeded the header size limit could cause Tomcat to treat a single
      2. request as multiple requests leading to the possibility of request
      3. smuggling when behind a reverse proxy.
      4. Users are recommended to upgrade to version 11.0.0-M11 onwards, 10.1.16 onwards, 9.0.83 onwards or 8.5.96 onwards, which fix the issue.
      5. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      6. CVSSv3:
      7. Base Score: HIGH (7.5)
      8. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      14. Vulnerable Software & Versions: (show all)
      15. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.83
      16. ...
    - CVE-2024-38286 suppress
      1. Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.
      2. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89. Older, unsupported versions may also be affected.
      3. Users are recommended to upgrade to version 11.0.0-M21, 10.1.25, or 9.0.90, which fixes the issue.
      4. Apache Tomcat, under certain configurations on any platform, allows an attacker to cause an OutOfMemoryError by abusing the TLS handshake process.
      5. CWE-770 Allocation of Resources Without Limits or Throttling
      6. CVSSv3:
      7. Base Score: HIGH (7.5)
      8. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. security@apache.org - MAILING\_LIST
      13. Vulnerable Software & Versions: (show all)
      14. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.13; versions up to (excluding) 9.0.90
      15. ...
    - CVE-2020-9484 suppress
      1. When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) 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; and d) 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. Note that all of conditions a) to d) must be true for the attack to succeed.
      2. CWE-502 Deserialization of Untrusted Data
      3. CVSSv3:
      4. Base Score: HIGH (7.0)
      5. Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.4)
      8. Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,MITIGATION,PATCH,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      21. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      22. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      23. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      24. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      25. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      26. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      27. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      28. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      29. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      30. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      31. security@apache.org - MAILING\_LIST,MITIGATION,PATCH,THIRD\_PARTY\_ADVISORY
      32. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      33. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      34. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      35. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      36. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      37. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      38. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      39. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      40. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      41. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      42. security@apache.org - THIRD\_PARTY\_ADVISORY
      43. security@apache.org - THIRD\_PARTY\_ADVISORY
      44. security@apache.org - THIRD\_PARTY\_ADVISORY
      45. security@apache.org - THIRD\_PARTY\_ADVISORY
      46. security@apache.org - THIRD\_PARTY\_ADVISORY
      47. security@apache.org - THIRD\_PARTY\_ADVISORY
      48. security@apache.org - THIRD\_PARTY\_ADVISORY
      49. security@apache.org - THIRD\_PARTY\_ADVISORY
      50. security@apache.org - THIRD\_PARTY\_ADVISORY
      51. security@apache.org - THIRD\_PARTY\_ADVISORY,VDB\_ENTRY
      52. Vulnerable Software & Versions: (show all)
      53. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.43
      54. ...
    - CVE-2021-25329 suppress
      1. The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: HIGH (7.0)
      5. Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.4)
      8. Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.41
      30. ...
    - CVE-2021-30640 suppress
      1. 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. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.
      2. CWE-116 Improper Encoding or Escaping of Output
      3. CVSSv3:
      4. Base Score: MEDIUM (6.5)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      21. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - THIRD\_PARTY\_ADVISORY
      24. security@apache.org - THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (excluding) 9.0.46
      30. ...
    - CVE-2022-34305 suppress
      1. In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.
      2. CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
      3. CVSSv3:
      4. Base Score: MEDIUM (6.1)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. security@apache.org - MAILING\_LIST,RELEASE\_NOTES,THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. security@apache.org - THIRD\_PARTY\_ADVISORY
      17. security@apache.org - THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions: (show all)
      19. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.30; versions up to (including) 9.0.64
      20. ...
    - CVE-2023-41080 suppress
      1. URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92.
      2. The vulnerability is limited to the ROOT (default) web application.
      3. CWE-601 URL Redirection to Untrusted Site ('Open Redirect')
      4. CVSSv3:
      5. Base Score: MEDIUM (6.1)
      6. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A
      7. References:
      8. af854a3a-2127-422b-91ae-364da2661108 - ISSUE\_TRACKING,PATCH,VENDOR\_ADVISORY
      9. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      13. security@apache.org - ISSUE\_TRACKING,PATCH,VENDOR\_ADVISORY
      14. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      15. security@apache.org - THIRD\_PARTY\_ADVISORY
      16. security@apache.org - THIRD\_PARTY\_ADVISORY
      17. security@apache.org - THIRD\_PARTY\_ADVISORY
      18. Vulnerable Software & Versions: (show all)
      19. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.79
      20. ...
    - CVE-2021-24122 suppress
      1. When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.
      2. CWE-706 Use of Incorrectly-Resolved Name or Reference, CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
      3. CVSSv3:
      4. Base Score: MEDIUM (5.9)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.3)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (including) 9.0.39
      22. ...
    - CVE-2021-33037 suppress
      1. Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 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. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: MEDIUM (5.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.0)
      8. Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. Vulnerable Software & Versions: (show all)
      31. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (excluding) 9.0.0; versions up to (including) 9.0.46
      32. ...
    - CVE-2023-42795 suppress
      1. Incomplete Cleanup vulnerability in Apache Tomcat.When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an error could
      2. cause Tomcat to skip some parts of the recycling process leading to
      3. information leaking from the current request/response to the next.
      4. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.
      5. CWE-459 Incomplete Cleanup
      6. CVSSv3:
      7. Base Score: MEDIUM (5.3)
      8. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. Vulnerable Software & Versions: (show all)
      21. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.81
      22. ...
    - CVE-2023-45648 suppress
      1. Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially
      2. crafted, invalid trailer header could cause Tomcat to treat a single
      3. request as multiple requests leading to the possibility of request
      4. smuggling when behind a reverse proxy.
      5. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.
      6. CWE-20 Improper Input Validation, NVD-CWE-Other
      7. CVSSv3:
      8. Base Score: MEDIUM (5.3)
      9. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A
      10. References:
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      16. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      17. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      18. security@apache.org - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - THIRD\_PARTY\_ADVISORY
      20. security@apache.org - VENDOR\_ADVISORY
      21. Vulnerable Software & Versions: (show all)
      22. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.81
      23. ...
    - CVE-2024-21733 suppress
      1. Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43.
      2. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.
      3. CWE-209 Generation of Error Message Containing Sensitive Information
      4. CVSSv3:
      5. Base Score: MEDIUM (5.3)
      6. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A
      7. References:
      8. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      9. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      10. security@apache.org - MAILING\_LIST,PATCH,THIRD\_PARTY\_ADVISORY
      11. security@apache.org - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      12. Vulnerable Software & Versions: (show all)
      13. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.1; versions up to (excluding) 9.0.44
      14. ...
    - CVE-2019-17569 suppress
      1. 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.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: MEDIUM (4.8)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      21. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      22. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. Vulnerable Software & Versions: (show all)
      29. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.28; versions up to (including) 9.0.30
      30. ...
    - CVE-2020-1935 suppress
      1. In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led 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.
      2. CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
      3. CVSSv3:
      4. Base Score: MEDIUM (4.8)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (5.8)
      8. Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - BROKEN\_LINK,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      17. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      18. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      19. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      20. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      21. security@apache.org - BROKEN\_LINK,MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      22. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      23. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      24. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      25. security@apache.org - THIRD\_PARTY\_ADVISORY
      26. security@apache.org - THIRD\_PARTY\_ADVISORY
      27. security@apache.org - THIRD\_PARTY\_ADVISORY
      28. security@apache.org - THIRD\_PARTY\_ADVISORY
      29. security@apache.org - THIRD\_PARTY\_ADVISORY
      30. security@apache.org - THIRD\_PARTY\_ADVISORY
      31. security@apache.org - THIRD\_PARTY\_ADVISORY
      32. Vulnerable Software & Versions: (show all)
      33. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.30
      34. ...
    - CVE-2020-13943 suppress
      1. If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 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. This could lead to users seeing responses for unexpected resources.
      2. NVD-CWE-noinfo
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A
      6. CVSSv2:
      7. Base Score: MEDIUM (4.0)
      8. Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N
      9. References:
      10. af854a3a-2127-422b-91ae-364da2661108 - BROKEN\_LINK
      11. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. af854a3a-2127-422b-91ae-364da2661108 - PATCH,THIRD\_PARTY\_ADVISORY
      13. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      14. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      15. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      16. af854a3a-2127-422b-91ae-364da2661108 - VENDOR\_ADVISORY
      17. security@apache.org - BROKEN\_LINK
      18. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      19. security@apache.org - PATCH,THIRD\_PARTY\_ADVISORY
      20. security@apache.org - THIRD\_PARTY\_ADVISORY
      21. security@apache.org - THIRD\_PARTY\_ADVISORY
      22. security@apache.org - THIRD\_PARTY\_ADVISORY
      23. security@apache.org - VENDOR\_ADVISORY
      24. Vulnerable Software & Versions: (show all)
      25. cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*
      26. ...
    - CVE-2023-28708 suppress
      1. When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.
      2. CWE-523 Unprotected Transport of Credentials
      3. CVSSv3:
      4. Base Score: MEDIUM (4.3)
      5. Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      8. security@apache.org - MAILING\_LIST,PATCH,VENDOR\_ADVISORY
      9. Vulnerable Software & Versions: (show all)
      10. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (excluding) 9.0.0; versions up to (excluding) 9.0.72
      11. ...
    - CVE-2021-43980 suppress
      1. The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client.
      2. CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
      3. CVSSv3:
      4. Base Score: LOW (3.7)
      5. Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:2.2/RC:R/MAV:A
      6. References:
      7. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      8. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      9. af854a3a-2127-422b-91ae-364da2661108 - MAILING\_LIST,VENDOR\_ADVISORY
      10. af854a3a-2127-422b-91ae-364da2661108 - THIRD\_PARTY\_ADVISORY
      11. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      12. security@apache.org - MAILING\_LIST,THIRD\_PARTY\_ADVISORY
      13. security@apache.org - MAILING\_LIST,VENDOR\_ADVISORY
      14. security@apache.org - THIRD\_PARTY\_ADVISORY
      15. Vulnerable Software & Versions: (show all)
      16. cpe:2.3:a:apache:tomcat:\*:\*:\*:\*:\*:\*:\*:\* versions from (including) 9.0.0; versions up to (including) 9.0.60
      17. ...

Non-Vulnerable

* classmate-1.5.1.jar
  + Library for introspecting types with full generic information including resolving of field and method types.
* jakarta.validation-api-2.0.2.jar
  + Jakarta Bean Validation API
* jboss-logging-3.4.1.Final.jar
  + The JBoss Logging Framework
* jul-to-slf4j-1.7.30.jar
  + JUL to SLF4J bridge
* log4j-to-slf4j-2.12.1.jar
  + The Apache Log4j binding between Log4j 2 API and SLF4J.
* slf4j-api-1.7.30.jar
  + The slf4j API
* tomcat-embed-el-9.0.30.jar
  + Core Tomcat implementation

# 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.

To begin we will start by first correcting the issues from the manual review with numerical correlation:

1. We will verifiy that the name parameter at @RequestParam is safe to utilize via validation. We can then explicitly clean the input or proved annotations such as @Valid.

2. We will correct the API security measures to include role-based access control and authentication tokens in the API security measures.

3. We will correct the lack of encryption by implementing and encryption procedure before storing or sending sensitive data.

4. To correct hardcoding sensitive data we will store them in remote environment variables or secured config files.

5. We will correct the stack traces issue by establishing a private log and giving a general error message that the user will see.

6. The int account\_balance field in customer class will be changed to private int account\_balance and as such we will also revise coding practices and procedures.

7. We will update the code quality by revising the .java names to follow correct scripting procedure.

Then we will correct the vulnerable dependencies mostly with updates as some can be easily corrected with newer versions that hold essential security updates or reviewing the risk factors of some of the dependencies that we can’t just simply update to see if we can prototype using a different proprietary that is more secure for our application needs.