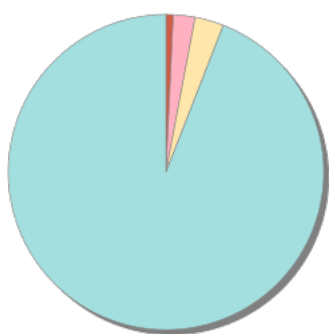# meterian

ASSESSMENT REPORT

Project: **cpass/cpassbe**
Branch: **mainline** (d8cd86b1799cc149e1ae3f970f0ac441d6c79696)
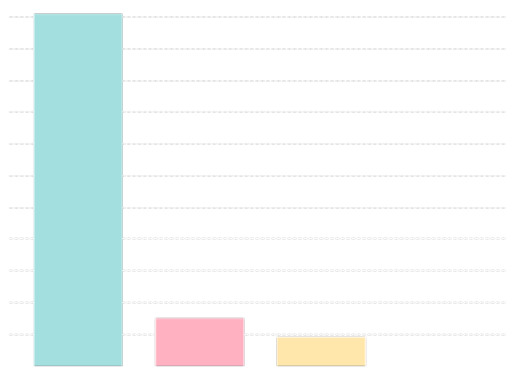
Created on **2025-05-23 08:31 UTC**
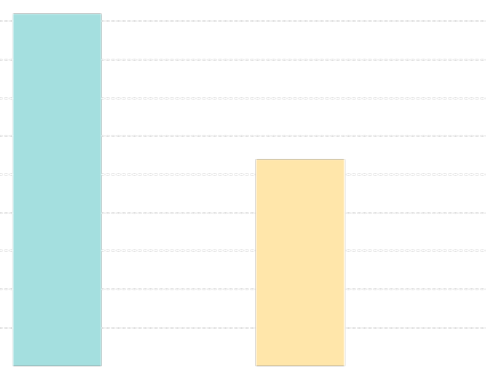
Security - 0

● CRITICAL ● HIGH ● MEDIUM ● LOW ● NONE

Stability - 85

■ UPDATED ■ PATCH ■ MINOR ■ MAJOR

Licensing - 73

■ VALID ■ FORBIDDEN ■ UNDECLARED ■ EXCLUDED

Security Assessment:
We have identified potential security issues in the libraries this project is using. You can find all the details in the security assessments below. While your code might not expose you to the security threat at the moment, it's recommended to go through each of them and update your libraries to a non-vulnerable version.
Score: 0

Stability Assessment:
There are new patch releases available for one or more of the project dependencies declared in this project. You will find all the details in the stability section below. It is recommended to update your dependencies to the latest patch release to benefit of all the latest bugfixes. While you are looking at it, consider also having a look at the new minor and major releases (in the same table) that can offer you more advanced features.
Score: 85

Licensing Assessment:
One or more of the project dependencies may be using a forbidden license. You will find all the details in the licensing assessment section below. We strongly advise you to not ship your software until such problem is resolved.
Score: 73

🛡 SECURITY ASSESSMENT

Library (java)

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: CRITICAL**

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariConfig.

More Info:

- https://access.redhat.com/errata/RHSA-2019:3200
- https://nvd.nist.gov/vuln/detail/CVE-2019-14540
- https://access.redhat.com/errata/RHSA-2020:0159
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: CRITICAL**

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-12814
- https://github.com/FasterXML/jackson-databind/issues/2341
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: CRITICAL

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the apache-log4j-extra (version 1.2.x) jar in the classpath, and an attacker can provide a JNDI service to access, it is possible to make the service execute a malicious payload.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-17531
- https://access.redhat.com/errata/RHSA-2020:0159
- https://access.redhat.com/errata/RHSA-2019:4192
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: CRITICAL

Description:

FasterXML jackson-databind 2.x before 2.9.9 might allow attackers to have a variety of impacts by leveraging failure to block the logback-core class from polymorphic deserialization. Depending on the classpath content, remote code execution may be possible.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-12384
- https://lists.debian.org/debian-lts-announce/2019/06/msg00019.html
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　**Severity: CRITICAL**

Description:

A flaw was discovered in FasterXML jackson-databind in all versions before 2.9.10 and 2.10.0, where it would permit polymorphic deserialization of malicious objects using the xalan JNDI gadget when used in conjunction with polymorphic type handling methods such as "enableDefaultTyping()" or when @JsonTypeInfo is using "Id.CLASS" or "Id.MINIMAL *CLASS" or in any other way which ObjectMapper.readValue might instantiate objects from unsafe sources. An attacker could use this flaw to execute arbitrary code.*

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-14893
- https://access.redhat.com/errata/RHSA-2020:0729
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14893
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　**Severity: CRITICAL**

Description:

A flaw was discovered in jackson-databind in versions before 2.9.10, 2.8.11.5 and 2.6.7.3, where it would permit polymorphic deserialization of a malicious object using commons-configuration 1 and 2 JNDI classes. An attacker could use this flaw to execute arbitrary code.

More Info:

- https://access.redhat.com/errata/RHSA-2020:0729
- https://nvd.nist.gov/vuln/detail/CVE-2019-14892
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14892
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　**Severity: CRITICAL**

Description:

FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2620
- http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200610-01-fastjason-en
- https://nvd.nist.gov/vuln/detail/CVE-2020-8840
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　**Severity: CRITICAL**

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.

More Info:

- https://access.redhat.com/errata/RHSA-2019:3200
- https://nvd.nist.gov/vuln/detail/CVE-2019-17267
- https://access.redhat.com/errata/RHSA-2020:0159
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　Severity: **CRITICAL**

Description:

SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is used (because of net.sf.ehcache.transaction.manager. DefaultTransactionManagerLookup), leading to remote code execution.

More Info:

- https://access.redhat.com/errata/RHBA-2019:2824
- https://nvd.nist.gov/vuln/detail/CVE-2019-14379
- http://seclists.org/fulldisclosure/2022/Mar/23
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　Severity: **CRITICAL**

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of org.apache.commons. dbcp.datasources.SharedPoolDataSource and org.apache.commons.dbcp.datasources. PerUserPoolDataSource mishandling.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-16942
- https://access.redhat.com/errata/RHSA-2019:3901
- https://access.redhat.com/errata/RHSA-2020:0159
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　**Severity: CRITICAL**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari. HikariConfig (aka shaded hikari-config).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-9546
- https://lists.apache.org/thread.html/ r35d30db00440ef63b791c4b7f7acb036e14d4a23afa2a249cb66c0fd%40%3Cissues. zookeeper.apache.org%3E
- https://github.com/FasterXML/jackson-databind/issues/2631
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　**Severity: CRITICAL**

Description:

FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-20330
- https://github.com/FasterXML/jackson-databind/issues/2526
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile) Severity: **CRITICAL**

Description:
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPConfig (aka anteros-core).

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-9548
- https://github.com/FasterXML/jackson-databind/issues/2634
- https://lists.apache.org/thread.html/ r35d30db00440ef63b791c4b7f7acb036e14d4a23afa2a249cb66c0fd%40%3Cissues. zookeeper.apache.org%3E
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile) Severity: **CRITICAL**

Description:
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy. P6DataSource mishandling.

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2019-16943
- https://access.redhat.com/errata/RHSA-2020:0160
- https://access.redhat.com/errata/RHSA-2020:0159
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: CRITICAL**

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariDataSource. This is a different vulnerability than CVE-2019-14540.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2019-16335
- https://access.redhat.com/errata/RHSA-2019:3200
- https://access.redhat.com/errata/RHSA-2020:0159
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: CRITICAL**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.ibatis.sqlmap.engine.transaction.jta. JtaTransactionConfig (aka ibatis-sqlmap).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-9547
- https://github.com/FasterXML/jackson-databind/issues/2634
- https://lists.apache.org/thread.html/
  r35d30db00440ef63b791c4b7f7acb036e14d4a23afa2a249cb66c0fd%40%3Cissues.
  zookeeper.apache.org%3E
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.aoju.bus.proxy.provider.remoting.RmiProvider (aka bus-proxy).

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-10968
- https://lists.debian.org/debian-lts-announce/2020/04/msg00012.html
- https://github.com/FasterXML/jackson-databind/issues/2662
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.openjpa.ee. WASRegistryManagedRuntime (aka openjpa).

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-11113
- https://lists.debian.org/debian-lts-announce/2020/04/msg00012.html
- https://github.com/FasterXML/jackson-databind/issues/2670
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.caucho.config.types.ResourceRef (aka caucho-quercus).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-10673
- https://github.com/FasterXML/jackson-databind/issues/2660
- https://lists.debian.org/debian-lts-announce/2020/03/msg00027.html
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to javax.swing.JEditorPane.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2642
- https://lists.debian.org/debian-lts-announce/2020/04/msg00012.html
- https://nvd.nist.gov/vuln/detail/CVE-2020-10969
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.proxy.provider.remoting. RmiProvider (aka apache/commons-proxy).

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-11112
- https://github.com/FasterXML/jackson-databind/issues/2666
- https://lists.debian.org/debian-lts-announce/2020/04/msg00012.html
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.aries.transaction.jms.internal. XaPooledConnectionFactory (aka aries.transaction.jms).

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-10672
- https://github.com/FasterXML/jackson-databind/issues/2659
- https://lists.debian.org/debian-lts-announce/2020/03/msg00027.html
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.activemq. **(aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).**

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-11111
- https://github.com/FasterXML/jackson-databind/issues/2664
- https://lists.debian.org/debian-lts-announce/2020/04/msg00012.html
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.commons.dbcp.cpdsadapter. DriverAdapterCPDS.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/3004
- https://nvd.nist.gov/vuln/detail/CVE-2020-36179
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　Severity: HIGH

Description:

A flaw was found in jackson-databind before 2.9.10.7. FasterXML mishandles the interaction between serialization gadgets and typing. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-20190
- https://bugzilla.redhat.com/show_bug.cgi?id=1916633
- https://github.com/FasterXML/jackson-databind/issues/2854
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)　　　　Severity: HIGH

Description:

FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oracle.jms.AQjmsQueueConnectionFactory, oracle.jms.AQjmsXATopicConnectionFactory, oracle.jms.AQjmsTopicConnectionFactory, oracle.jms.AQjmsXAQueueConnectionFactory, and oracle.jms.AQjmsXAConnectionFactory (aka weblogic/oracle-aqjms).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-14061
- https://lists.debian.org/debian-lts-announce/2020/07/msg00001.html
- https://github.com/FasterXML/jackson-databind/issues/2698
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
　　org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
　　　　com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.6 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPDataSource (aka Anteros-DBCP).

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2814
- https://lists.debian.org/debian-lts-announce/2021/04/msg00025.html
- https://nvd.nist.gov/vuln/detail/CVE-2020-24616
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to com.sun.org.apache.xalan.internal.lib.sql. JNDIConnectionPool (aka xalan2).

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2704
- https://lists.debian.org/debian-lts-announce/2020/07/msg00001.html
- https://nvd.nist.gov/vuln/detail/CVE-2020-14062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.6 mishandles the interaction between serialization gadgets and typing, related to com.pastdev.httpcomponents.configuration. JndiConfiguration.

More Info:
- https://github.com/FasterXML/jackson-databind/commit/ad5a630174f08d279504bc51ebba8772fd71b86b
- https://github.com/FasterXML/jackson-databind/issues/2798
- https://nvd.nist.gov/vuln/detail/CVE-2020-24750
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources. SharedPoolDataSource.

More Info:
- https://github.com/FasterXML/jackson-databind/issues/2997
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- https://nvd.nist.gov/vuln/detail/CVE-2020-36187
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db. DriverManagerConnectionSource.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2996
- https://nvd.nist.gov/vuln/detail/CVE-2020-36189
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources. PerUserPoolDataSource.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2998
- https://nvd.nist.gov/vuln/detail/CVE-2020-36184
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.cpdsadapter. DriverAdapterCPDS.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-36182
- https://github.com/FasterXML/jackson-databind/issues/3004
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources. PerUserPoolDataSource.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2997
- https://nvd.nist.gov/vuln/detail/CVE-2020-36186
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.docx4j.org.apache.xalan.lib.sql. JNDIConnectionPool.

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-36183
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- https://github.com/FasterXML/jackson-databind/issues/3003
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.cpdsadapter. DriverAdapterCPDS.

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-36181
- https://github.com/FasterXML/jackson-databind/issues/3004
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.oracle.wls.shaded.org.apache.xalan.lib.sql. JNDIConnectionPool (aka embedded Xalan in org.glassfish.web/javax.servlet.jsp.jstl).

More Info:

- https://lists.debian.org/debian-lts-announce/2021/04/msg00025.html
- https://github.com/FasterXML/jackson-databind/issues/2999
- https://nvd.nist.gov/vuln/detail/CVE-2020-35728
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

A deserialization flaw was discovered in jackson-databind through 2.9.10.4. It could allow an unauthenticated user to perform code execution via ignite-jta or quartz-core: org.apache. ignite.cache.jta.jndi.CacheJndiTmLookup, org.apache.ignite.cache.jta.jndi. CacheJndiTmFactory, and org.quartz.utils.JNDIConnectionProvider.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-10650
- https://github.com/FasterXML/jackson-databind/commit/ a424c038ba0c0d65e579e22001dec925902ac0ef
- https://github.com/advisories/GHSA-rpr3-cw39-3pxh
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db. JNDIConnectionSource.

More Info:
- https://github.com/FasterXML/jackson-databind/issues/2996
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- https://nvd.nist.gov/vuln/detail/CVE-2020-36188
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.cpdsadapter. DriverAdapterCPDS.

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2020-36180
- https://github.com/FasterXML/jackson-databind/issues/3004
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: HIGH

Description:

FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.xalan.lib.sql. JNDIConnectionPool (aka apache/drill).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-14060
- https://lists.debian.org/debian-lts-announce/2020/07/msg00001.html
- https://github.com/FasterXML/jackson-databind/issues/2688
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: HIGH

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.springframework.aop.config. MethodLocatingFactoryBean (aka spring-aop).

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2680
- https://nvd.nist.gov/vuln/detail/CVE-2020-11619
- https://lists.apache.org/thread.html/
  rf1bbc0ea4a9f014cf94df9a12a6477d24a27f52741dbc87f2fd52ff2%40%3Cissues.geode.
  apache.org%3E
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: HIGH

Description:

FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.jelly.impl.Embedded (aka commons-jelly).

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-11620
- https://lists.apache.org/thread.html/ rf1bbc0ea4a9f014cf94df9a12a6477d24a27f52741dbc87f2fd52ff2%40%3Cissues.geode. apache.org%3E
- https://github.com/FasterXML/jackson-databind/issues/2682
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: HIGH

Description:

FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to org.jsecurity.realm.jndi.JndiRealmFactory (aka org.jsecurity).

More Info:

- https://lists.debian.org/debian-lts-announce/2020/07/msg00001.html
- https://github.com/FasterXML/jackson-databind/issues/2765
- https://nvd.nist.gov/vuln/detail/CVE-2020-14195
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources. PerUserPoolDataSource.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2986
- https://nvd.nist.gov/vuln/detail/CVE-2020-35490
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources. SharedPoolDataSource.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2986
- https://nvd.nist.gov/vuln/detail/CVE-2020-35491
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources. SharedPoolDataSource.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2998
- https://nvd.nist.gov/vuln/detail/CVE-2020-36185
- https://cowtowncoder.medium.com/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

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.*

More Info:

- https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490
- https://nvd.nist.gov/vuln/detail/CVE-2022-42004
- https://github.com/FasterXML/jackson-databind/commit/063183589218fec19a9293ed2f17ec53ea80ba88
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9.2. This occurs when Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the logback jar in the classpath.

More Info:

- https://github.com/FasterXML/jackson-databind/commit/ ad418eeb974e357f2797aef64aa0e3ffaaa6125b
- https://access.redhat.com/errata/RHSA-2019:3200
- https://nvd.nist.gov/vuln/detail/CVE-2019-14439
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.

More Info:

- https://github.com/FasterXML/jackson-databind/issues/2816
- https://nvd.nist.gov/vuln/detail/CVE-2020-36518
- https://lists.debian.org/debian-lts-announce/2022/05/msg00001.html
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

All versions of 2.x through 2.6.7.2, versions between 2.7.0 and 2.8.11.5, and all versions of 2.9.x through 2.9.9 are vulnerable to Deserialization of Untrusted Data.

Users should update to either 2.6.7.3, 2.8.11.5 or 2.9.0,2.9.10

More Info:

- https://github.com/FasterXML/jackson-databind/commit/ d4983c740fec7d5576b207a8c30a63d3ea7443de
- https://github.com/FasterXML/jackson-databind/issues/2420
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

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.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-25649
- https://bugzilla.redhat.com/show_bug.cgi?id=1887664
- https://github.com/FasterXML/jackson-databind/issues/2589
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0

org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final

com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: HIGH**

Description:

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.*

More Info:

- https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020
- https://github.com/FasterXML/jackson-databind/commit/d78d00ee7b5245b93103fef3187f70543d67ca33
- https://nvd.nist.gov/vuln/detail/CVE-2022-42003
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
      org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
            com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   **Severity: MEDIUM**

Description:

Vulnerable versions of this library are affected by CWE-787: Out-of-bounds Write

More Info:

- https://github.com/FasterXML/jackson-databind/issues/3328
- https://github.com/FasterXML/jackson-databind/commit/3ccde7d938fea547e598fdefe9a82cff37fed5cb
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
      org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
            com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile) **Severity: MEDIUM**

Description:

Vulnerable versions of this library are affected by CWE-400: Uncontrolled Resource
Consumption

More Info:

- https://github.com/FasterXML/jackson-databind/commit/
  7c0a74ee77a0896e9a3fde3600066ea0b7490f5b
- https://github.com/FasterXML/jackson-databind/issues/3655
- https://github.com/FasterXML/jackson-databind/pull/3666
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
  org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
    com.fasterxml.jackson.core:jackson-databind:2.9.9

---

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile) **Severity: SUGGEST**

Description:

Vulnerable versions of this library are affected by CWE-400: Uncontrolled Resource
Consumption

More Info:

- https://github.com/FasterXML/jackson-databind/commit/
  80d9b522b3bd75c6f42651c649d0d0736038e5ac
- https://github.com/FasterXML/jackson-databind/issues/2501
- https://github.com/FasterXML/jackson-databind/commit/
  4ea844d6112b2b203ae2c8d5740c8b0a5e7c2d1c
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
  org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
    com.fasterxml.jackson.core:jackson-databind:2.9.9

com.fasterxml.jackson.core:jackson-databind - 2.9.9 (compile)   Severity: SUGGEST

Description:

The error can be found in any recursively-typed data structure. It is not a Jackson library-specific issue. Jackson will not find any loops in the data structure. The same thing would happen if hashCode were to be called in the same map. This would also result in a stack overflow. However, this is not considered to be a security concern.

The report does not provide any evidence of how this issue could be used for a DDoS attack via a built-in string.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2023-35116
- https://github.com/FasterXML/jackson-databind/issues/3972
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.fasterxml.jackson.core:jackson-databind:2.9.9

com.google.guava:guava - 25.0-jre (compile)   Severity: HIGH

Description:

Use of Java's default temporary directory for file creation in "FileBackedOutputStream" in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class.

Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.

More Info:

- https://github.com/google/guava/issues/2575
- https://nvd.nist.gov/vuln/detail/CVE-2023-2976
- https://security.netapp.com/advisory/ntap-20230818-0008/
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.github.fge:json-patch:1.3
            com.github.fge:jackson-coreutils:1.0
                com.google.guava:guava:25.0-jre

com.google.guava:guava - 25.0-jre (compile)   Severity: **LOW**

Description:
A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir(). By default, on unix-like systems, the created directory is world-readable (readable by an attacker with access to the system). The method in question has been marked @Deprecated in versions 30.0 and later and should not be used. For Android developers, we recommend choosing a temporary directory API provided by Android, such as context.getCacheDir(). For other Java developers, we recommend migrating to the Java 7 API java.nio.file.Files.createTempDirectory() which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.

More Info:
- https://github.com/google/guava/commit/fec0dbc4634006a6162cfd4d0d09c962073ddf40
- https://nvd.nist.gov/vuln/detail/CVE-2020-8908
- https://github.com/google/guava/issues/4011
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-jackson2-provider:3.7.0.Final
        com.github.fge:json-patch:1.3
            com.github.fge:jackson-coreutils:1.0
                com.google.guava:guava:25.0-jre

com.squareup.okio:okio - 1.6.0 (provided)   Severity: **HIGH**

Description:
GzipSource does not handle an exception that might be raised when parsing a malformed gzip buffer. This may lead to denial of service of the Okio client when handling a crafted GZIP archive, by using the GzipSource class.

More Info:
- https://nvd.nist.gov/vuln/detail/CVE-2023-3635
- https://github.com/square/okio/commit/81bce1a30af244550b0324597720e4799281da7b
- https://research.jfrog.com/vulnerabilities/okio-gzip-source-unhandled-exception-dos-xray-523195/
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    it.csi.cpass:cpassbe-ejb:2.1.0
        com.squareup.okhttp:okhttp:2.7.5
            com.squareup.okio:okio:1.6.0

commons-io:commons-io - 2.5 (provided)   Severity: MEDIUM

Description:
Uncontrolled Resource Consumption vulnerability in Apache Commons IO.
The "org.apache.commons.io.input.XmlStreamReader" class may excessively consume CPU resources when processing maliciously crafted input.
This issue affects Apache Commons IO: from 2.0 before 2.14.0.
Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.

More Info:
- https://github.com/advisories/GHSA-78wr-2p64-hpwj
- https://github.com/apache/commons-io
- https://nvd.nist.gov/vuln/detail/CVE-2024-47554
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-integ-stilo:2.1.0
    it.csi.cpass:cpassbe-lib:2.1.0
        commons-io:commons-io:2.5

commons-io:commons-io - 2.5 (provided)   Severity: MEDIUM

Description:
In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

More Info:
- https://issues.apache.org/jira/browse/IO-556
- https://lists.apache.org/thread.html/
  r01b4a1fcdf3311c936ce33d75a9398b6c255f00c1a2f312ac21effe1%40%3Cnotifications.
  zookeeper.apache.org%3E
- https://nvd.nist.gov/vuln/detail/CVE-2021-29425
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-integ-stilo:2.1.0
    it.csi.cpass:cpassbe-lib:2.1.0
        commons-io:commons-io:2.5

org.apache.httpcomponents:httpclient - 4.5.4 (provided)   **Severity: MEDIUM**

Description:

Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the library as java.net.URI object and pick the wrong target host for request execution.

More Info:

- https://lists.apache.org/thread.html/ r03bbc318c81be21f5c8a9b85e34f2ecc741aa804a8e43b0ef2c37749%40%3Cissues. maven.apache.org%3E
- https://nvd.nist.gov/vuln/detail/CVE-2020-13956
- https://lists.apache.org/thread.html/ r043a75acdeb52b15dd5e9524cdadef4202e6a5228644206acf9363f9%40%3Cdev.hive. apache.org%3E
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    it.csi.cpass:cpassbe-ejb:2.1.0
        org.apache.httpcomponents:httpclient:4.5.4

---

org.apache.james:apache-mime4j - 0.6 (provided)   **Severity: MEDIUM**

Description:

Unproper laxist permissions on the temporary files used by MIME4J TempFileStorageProvider may lead to information disclosure to other local users. This issue affects Apache James MIME4J version 0.8.8 and prior versions. We recommend users to upgrade to MIME4j version 0.8.9 or later.

More Info:

- https://github.com/advisories/GHSA-q84x-3476-8ff2
- https://nvd.nist.gov/vuln/detail/CVE-2022-45787
- https://lists.apache.org/thread/26s8p9stl1z261c4qw15bsq03tt7t0rj
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-multipart-provider:3.7.0.Final
        org.apache.james:apache-mime4j:0.6

org.jboss.resteasy:resteasy-client - 3.7.0.Final (provided)   **Severity: HIGH**

Description:
A flaw was found in all resteasy 3.x.x versions prior to 3.12.0.Final and all resteasy 4.x.x versions prior to 4.6.0.Final, where an improper input validation results in returning an illegal header that integrates into the server's response. This flaw may result in an injection, which leads to unexpected behavior when the HTTP response is constructed.

More Info:
- https://github.com/resteasy/Resteasy/commit/ 88ba8537f2e8d465c7031d352bf9bb25526ce475
- https://nvd.nist.gov/vuln/detail/CVE-2020-1695
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1695
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-multipart-provider:3.7.0.Final
        org.jboss.resteasy:resteasy-client:3.7.0.Final

---

org.jboss.resteasy:resteasy-client - 3.7.0.Final (provided)   **Severity: MEDIUM**

Description:
A flaw was found in RESTEasy where the endpoint class and method names are returned as part of the exception response when RESTEasy cannot convert one of the request URI path or query values to the matching JAX-RS resource method's parameter value. The highest threat from this vulnerability is to data confidentiality.

More Info:
- https://gitlab.com/gitlab-org/advisories-community/-/blob/main/maven/org.jboss.resteasy/ resteasy-client/CVE-2021-20289.yml
- https://bugzilla.redhat.com/show_bug.cgi?id=1935927
- https://nvd.nist.gov/vuln/detail/CVE-2021-20289
- (registry)

Locations:
/pom.xml

Hierarchy:
it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-multipart-provider:3.7.0.Final
        org.jboss.resteasy:resteasy-client:3.7.0.Final

org.jboss.resteasy:resteasy-client - 3.7.0.Final (provided)   **Severity: MEDIUM**

Description:

A flaw was found in RESTEasy client in all versions of RESTEasy up to 4.5.6.Final. It may allow client users to obtain the server's potentially sensitive information when the server got WebApplicationException from the RESTEasy client call. The highest threat from this vulnerability is to data confidentiality.

More Info:

- https://nvd.nist.gov/vuln/detail/CVE-2020-25633
- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-25633
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-multipart-provider:3.7.0.Final
        org.jboss.resteasy:resteasy-client:3.7.0.Final

---

org.jboss.resteasy:resteasy-jaxrs - 3.7.0.Final (provided)   **Severity: MEDIUM**

Description:

A cross-site scripting (XSS) flaw was found in RESTEasy where it does not properly handle URL encoding when the "RESTEASY003870" exception occurs. An attacker could use this flaw to launch a reflected XSS attack.

More Info:

- https://bugzilla.redhat.com/show_bug.cgi?id=1814974
- https://nvd.nist.gov/vuln/detail/CVE-2020-10688
- https://github.com/quarkusio/quarkus/issues/7248
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-multipart-provider:3.7.0.Final
        org.jboss.resteasy:resteasy-jaxrs:3.7.0.Final

org.jboss.resteasy:resteasy-jaxrs - 3.7.0.Final (provided)   **Severity: MEDIUM**

Description:

A flaw was found in RESTEasy where the endpoint class and method names are returned as part of the exception response when RESTEasy cannot convert one of the request URI path or query values to the matching JAX-RS resource method's parameter value. The highest threat from this vulnerability is to data confidentiality.

More Info:

- https://bugzilla.redhat.com/show_bug.cgi?id=1935927
- https://nvd.nist.gov/vuln/detail/CVE-2021-20289
- https://gitlab.com/gitlab-org/advisories-community/-/blob/main/maven/org.jboss.resteasy/resteasy-jaxrs/CVE-2021-20289.yml
- (registry)

Locations:

/pom.xml

Hierarchy:

it.csi.cpass:cpassbe-web:2.1.0
    org.jboss.resteasy:resteasy-multipart-provider:3.7.0.Final
        org.jboss.resteasy:resteasy-jaxrs:3.7.0.Final

STABILITY ASSESSMENT

Libraries (java)

com.google.code.gson:gson 2.8.9 (compile)
new patch release: **2.8.9**
new minor release: **2.13.1**

(registry)

com.opencsv:opencsv 5.3 (compile)
new minor release: **5.10**

(registry)

commons-io:commons-io 2.5 (compile)
new minor release: **2.19.0**

(registry)

io.gsonfire:gson-fire 1.8.0 (compile)
new patch release: **1.8.5**
new minor release: **1.9.0**

(registry)

io.swagger:swagger-annotations 1.5.18 (compile)
new patch release: **1.5.24**
new minor release: **1.6.16**

(registry)

javax.cache:cache-api 1.0.0 (compile)
new patch release: **1.0.0-PFD**
new minor release: **1.1.1**

(registry)

joda-time:joda-time 2.9.7 (compile)
new patch release: **2.9.9**
new minor release: **2.14.0**

(registry)

junit:junit 4.12 (test)
new minor release: **4.13.2**

(registry)

org.apache.commons:commons-text 1.10.0 (compile)
new patch release: **1.10.0**
new minor release: **1.13.1**

(registry)

org.apache.httpcomponents:httpclient 4.5.4 (compile)
new patch release: **4.5.14**

(registry)

org.apache.httpcomponents:httpmime 4.5.13 (compile)
new patch release: **4.5.14**

(registry)

org.apache.logging.log4j:log4j-api 2.17.0 (compile)
new patch release: **2.17.2**
new minor release: **2.24.3**

(registry)

org.apache.logging.log4j:log4j-to-slf4j 2.17.0 (compile)
new patch release: **2.17.2**
new minor release: **2.24.3**

(registry)

org.jboss.arquillian.junit:arquillian-junit-container 1.4.0.Final (test)
new patch release: **1.4.1.Final**
new minor release: **1.9.4.Final**

(registry)

org.jboss.arquillian.protocol:arquillian-protocol-servlet 1.4.0.Final (test)
new patch release: **1.4.1.Final**
new minor release: **1.9.4.Final**

(registry)

org.jboss.ejb3:jboss-ejb3-ext-api 2.3.0.Final (compile)
new patch release: **2.3.0.Final**
new minor release: **2.4.0.Final**

(registry)

org.jboss.resteasy:resteasy-jackson2-provider 3.7.0.Final (compile)
new patch release: **3.7.0.Final**
new minor release: **3.15.6.Final**
New major release: **6.2.12.Final**

(registry)

org.jboss.resteasy:resteasy-multipart-provider 3.7.0.Final (provided)
new patch release: **3.7.0.Final**
new minor release: **3.15.6.Final**
New major release: **6.2.12.Final**

(registry)

org.jboss.shrinkwrap.resolver:shrinkwrap-resolver-bom 2.1.1 (test)
new patch release: **2.1.1**
new minor release: **2.2.7**
New major release: **3.3.4**

(registry)

org.jboss.shrinkwrap.resolver:shrinkwrap-resolver-impl-maven 2.2.6 (test)
new patch release: **2.2.7**
New major release: **3.3.4**

(registry)

org.jboss.shrinkwrap.resolver:shrinkwrap-resolver-impl-maven-archive 2.2.6 (test)
new patch release: **2.2.7**
New major release: **3.3.4**

(registry)

org.mapstruct:mapstruct 1.4.1.Final (compile)
new patch release: **1.4.2.Final**
new minor release: **1.6.3**

(registry)

org.postgresql:postgresql 42.7.3 (test)
new patch release: **42.7.5**

(registry)

org.threeten:threetenbp 1.3.5 (compile)
new patch release: **1.3.8**
new minor release: **1.7.1**

(registry)

📗 LICENSING ASSESSMENT

Libraries (java)

❓ it.csi.cpass:cpassbe-angular 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-ear 2.1.0 (compile)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-ejb 2.1.0 (provided)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-exposed 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-integ-acta 2.1.0 (compile)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-integ-hr 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-integ-notier 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-integ-siac 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-integ-sicraweb 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-integ-stilo 2.1.0 (root)
    We were not able to find a valid license.
(registry)

❓ it.csi.cpass:cpassbe-lib 2.1.0 (provided)
    We were not able to find a valid license.
(registry)

it.csi.cpass:cpassbe-tar 2.1.0 (root)
We were not able to find a valid license.
(registry)

it.csi.cpass:cpassbe-web 2.1.0 (root)
We were not able to find a valid license.
(registry)

com.fasterxml.jackson.core:jackson-annotations 2.9.9 (compile) (transitive)
Apache-2.0
(registry)

com.fasterxml.jackson.core:jackson-core 2.9.9 (compile) (transitive)
Apache-2.0
(registry)

com.fasterxml.jackson.core:jackson-databind 2.9.9 (compile) (transitive)
Apache-2.0
LGPL-3.0-only
(registry)

com.fasterxml.jackson.jaxrs:jackson-jaxrs-base 2.9.9 (compile) (transitive)
Apache-2.0
(registry)

com.fasterxml.jackson.jaxrs:jackson-jaxrs-json-provider 2.9.9 (compile) (transitive)
Apache-2.0
(registry)

com.fasterxml.jackson.module:jackson-module-jaxb-annotations 2.9.9 (compile) (transitive)
Apache-2.0
(registry)

com.github.fge:jackson-coreutils 1.0 (compile) (transitive)
LGPL-2.1-only
(registry)

com.github.fge:json-patch 1.3 (compile) (transitive)
LGPL-2.1-only
(registry)

com.google.code.gson:gson 2.8.9 (provided) (transitive)
Apache-2.0
(registry)

com.google.guava:guava 25.0-jre (compile) (transitive)
Apache-2.0
(registry)

✅ com.opencsv:opencsv 5.3 (provided) (transitive)
Apache-2.0
(registry)

✅ com.squareup.okhttp:logging-interceptor 2.7.5 (provided) (transitive)
Apache-2.0
(registry)

✅ com.squareup.okhttp:okhttp 2.7.5 (provided) (transitive)
Apache-2.0
(registry)

✅ com.squareup.okio:okio 1.6.0 (provided) (transitive)
Apache-2.0
(registry)

✅ com.sun.mail:javax.mail 1.6.2 (provided) (transitive)
CDDL-1.1
(registry)

✅ commons-beanutils:commons-beanutils 1.9.4 (provided) (transitive)
Apache-2.0
(registry)

✅ commons-codec:commons-codec 1.11 (provided) (transitive)
Apache-2.0
(registry)

✅ commons-collections:commons-collections 3.2.2 (provided) (transitive)
Apache-2.0
(registry)

✅ commons-io:commons-io 2.5 (provided)
Apache-2.0
(registry)

✅ commons-lang:commons-lang 2.6 (provided) (transitive)
Apache-2.0
(registry)

✅ commons-logging:commons-logging 1.2 (provided) (transitive)
Apache-2.0
(registry)

✅ io.gsonfire:gson-fire 1.8.0 (provided) (transitive)
MIT
(registry)

✅ io.swagger:swagger-annotations 1.5.18 (provided) (transitive)
    Apache-2.0
(registry)

✅ javax.activation:activation 1.1.1 (provided) (transitive)
    CDDL-1.0
(registry)

✅ javax.activation:javax.activation-api 1.2.0 (provided) (transitive)
    CDDL-1.1
(registry)

✅ javax.annotation:javax.annotation-api 1.3.2 (provided) (transitive)
    CDDL-1.1
    Apache-2.0
(registry)

✅ javax.cache:cache-api 1.0.0 (provided) (transitive)
    Apache-2.0
(registry)

✅ javax.jws:javax.jws-api 1.1 (provided)
    CDDL-1.1
(registry)

✅ javax.validation:validation-api 2.0.1.Final (provided) (transitive)
    Apache-2.0
(registry)

✅ javax.xml.bind:jaxb-api 2.4.0-b180830.0359 (provided) (transitive)
    CDDL-1.1
(registry)

✅ javax.xml.soap:javax.xml.soap-api 1.4.0 (provided) (transitive)
    Apache-2.0
(registry)

✅ javax.xml.ws:jaxws-api 2.3.1 (provided)
    CDDL
    GPL-2.0
    Apache-2.0
(registry)

✅ javax:javaee-api 8.0.1 (provided)
    CDDL-1.1
(registry)

✅ javax:javaee-web-api 8.0.1 (provided)
    CDDL-1.1
(registry)

✅ joda-time:joda-time 2.9.7 (provided) (transitive)
   Apache-2.0
(registry)

✅ net.jcip:jcip-annotations 1.0 (compile) (transitive)
   BSD
(registry)

✅ org.apache.commons:commons-collections4 4.4 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.commons:commons-lang3 3.11 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.commons:commons-lang3 3.12.0 (compile) (transitive)
   Apache-2.0
(registry)

✅ org.apache.commons:commons-text 1.10.0 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.httpcomponents:httpclient 4.5.4 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.httpcomponents:httpcore 4.4.5 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.httpcomponents:httpmime 4.5.13 (compile)
   Apache-2.0
(registry)

✅ org.apache.james:apache-mime4j 0.6 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.logging.log4j:log4j-api 2.17.0 (provided) (transitive)
   Apache-2.0
(registry)

✅ org.apache.logging.log4j:log4j-to-slf4j 2.17.0 (provided) (transitive)
   Apache-2.0
(registry)

---

org.jboss.ejb3:jboss-ejb3-ext-api 2.3.0.Final (provided) (transitive)

PUBDOM

(registry)

org.jboss.logging:jboss-logging 3.4.0.Final (compile) (transitive)

Apache-2.0

(registry)

org.jboss.resteasy:resteasy-client 3.7.0.Final (provided) (transitive)

Apache-2.0

(registry)

org.jboss.resteasy:resteasy-jackson2-provider 3.7.0.Final (compile)

Apache-2.0

(registry)

org.jboss.resteasy:resteasy-jaxb-provider 3.7.0.Final (provided) (transitive)

Apache-2.0

(registry)

org.jboss.resteasy:resteasy-jaxrs 3.7.0.Final (provided) (transitive)

Apache-2.0

(registry)

org.jboss.resteasy:resteasy-multipart-provider 3.7.0.Final (provided)

Apache-2.0

(registry)

org.jboss.spec.javax.annotation:jboss-annotations-api_1.3_spec 1.0.1.Final (provided) (transitive)

CDDL-1.1

(registry)

org.jboss.spec.javax.ws.rs:jboss-jaxrs-api_2.1_spec 1.0.2.Final (provided) (transitive)

CDDL-1.0

GPL-2.0-only

(registry)

org.jboss.spec.javax.xml.bind:jboss-jaxb-api_2.3_spec 1.0.1.Final (provided) (transitive)

CDDL-1.1

(registry)

org.mapstruct:mapstruct 1.4.1.Final (provided)

Apache-2.0

(registry)

org.reactivestreams:reactive-streams 1.0.2 (provided) (transitive)

CC0-1.0

(registry)

✅ org.slf4j:slf4j-api 1.7.22.jbossorg-1 (provided) (transitive)
    MIT
(registry)

✅ org.threeten:threetenbp 1.3.5 (provided) (transitive)
    BSD-3-Clause
(registry)