Security Export

Fri Sep 8, 2023

Exported by: vtekal

Package type: Docker

Component name: linkedin/datahub-gms:sha256__21e522d1168912ec1795307b6f6897d6110b2d169656adb849e2ec184f44ea73

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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.	CVE-2019-16943	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the openjpa class from polymorphic deserialization.	CVE-2018-19361	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2023-04-16T02:26:03-05:00
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.	CVE-2020-8840	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.	CVE-2019-17267	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the blaze-ds-opt and blaze-ds-core classes from polymorphic deserialization.	CVE-2018-14719	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2022-11-15T01:26:03-06:00
FasterXML jackson-databind before 2.7.9.3, 2.8.x before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath.	CVE-2018-7489	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.1,1.9.13-cloudera.1	2022-11-15T01:26:03-06:00
FasterXML jackson-databind 2.x before 2.9.7 might allow attackers to conduct external XML entity (XXE) attacks by leveraging failure to block unspecified JDK classes from polymorphic deserialization.	CVE-2018-14720	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2022-12-26T01:26:17-06:00
A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariConfig.	CVE-2019-14540	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to conduct server-side request forgery (SSRF) attacks by leveraging failure to block the axis2-jaxws class from polymorphic deserialization.	CVE-2018-14721	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2023-04-16T02:26:03-05:00
A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike.	CVE-2019-10202	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	<= 1.9.13		2023-07-18T02:26:10-05:00
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).	CVE-2020-9547	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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.	CVE-2019-16942	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the jboss-common-core class from polymorphic deserialization.	CVE-2018-19362	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2023-04-16T02:26:03-05:00
FasterXML jackson-databind through 2.8.10 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the Spring libraries are available in the classpath.	CVE-2017-17485	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.1,1.9.13-cloudera.1	2022-11-15T01:26:03-06:00
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.	CVE-2019-14892	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the slf4j-ext class from polymorphic deserialization.	CVE-2018-14718	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2022-11-15T01:26:03-06:00
FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.	CVE-2019-20330	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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.	CVE-2019-14893	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the axis2-transport-jms class from polymorphic deserialization.	CVE-2018-19360	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.2,1.9.13-cloudera.2	2023-04-16T02:26:03-05:00
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).	CVE-2020-9548	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2016-1000027	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/spring-web-5.3.29.jar	org.springframework:spring-web	< 6.0.0	6.0.0	2023-01-10T01:26:36-06:00
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.	CVE-2019-14379	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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).	CVE-2020-9546	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2019-16335	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.	CVE-2017-7525	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.1,1.9.13-cloudera.1	2022-11-15T01:26:03-06:00
A deserialization flaw was discovered in the jackson-databind in versions before 2.8.10 and 2.9.1, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.	CVE-2017-15095	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.1,1.9.13-cloudera.1	2023-04-16T02:26:03-05:00
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.	CVE-2019-17531	Critical	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-35490	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-14062	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Apache Lucene Operations Class Improper Regular Expression Handling CPU Consumption Remote DoS		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/lucene-analyzers-common-8.7.0.jar	org.apache.lucene:lucene-analyzers-common	< 8.10.0	8.10.0,9.0.0	2022-04-12T21:26:13-05:00
Apache Lucene Operations Class Improper Regular Expression Handling CPU Consumption Remote DoS		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/lucene-queryparser-8.7.0.jar	org.apache.lucene:lucene-queryparser	< 8.10.0	8.10.0,9.0.0	2022-04-12T21:26:13-05:00
Apache Lucene Operations Class Improper Regular Expression Handling CPU Consumption Remote DoS		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/lucene-sandbox-8.7.0.jar	org.apache.lucene:lucene-sandbox	< 8.10.0	8.10.0,9.0.0	2022-04-12T21:26:13-05:00
Apache Lucene Operations Class Improper Regular Expression Handling CPU Consumption Remote DoS		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/lucene-suggest-8.7.0.jar	org.apache.lucene:lucene-suggest	< 8.10.0	8.10.0,9.0.0	2022-04-12T21:26:13-05:00
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.	CVE-2020-36179	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-36180	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-35728	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

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.

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
	CVE-2023-2976	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/graphql-java-19.5.jar/META-INF/maven/com.google.guava/guava/pom.xml	com.google.guava:guava	< 32.0.1-jre	32.0.1-android,32.0.1-jre	2023-08-25T02:26:05-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Elasticsearch Improper API Key Authorization Remove API Key Use	CVE-2021-22149	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/elasticsearch-7.10.2.jar	org.elasticsearch:elasticsearch	< 7.14.0	7.14.0	2021-11-13T04:47:32-06:00
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.	CVE-2020-36186	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-10672	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-14061	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
** DISPUTED ** The web-based admin console in H2 Database Engine through 2.1.214 can be started via the CLI with the argument -webAdminPassword, which allows the user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that has obtained local access through some means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states "This is not a vulnerability of H2 Console ... Passwords should never be passed on the command line and every qualified DBA or system administrator is expected to know that."	CVE-2022-45868	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/h2-2.1.214.jar	com.h2database:h2	< 2.2.220	2.2.220	2023-07-20T02:26:03-05:00
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).	CVE-2020-11620	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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.	CVE-2019-14439	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
Oracle MySQL Connector/J JDBC Connection Handling Insecure Deserialization Arbitrary Code Execution Weakness		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/mysql-connector-java-8.0.20.jar	mysql:mysql-connector-java	3.1.5 <= Version <= 8.0.26		2021-11-13T04:47:33-06:00
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.	CVE-2020-24750	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-11111	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-24616	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-10673	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-36185	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
There exists an vulnerability causing an abort() to be called in gRPC.ï¿½ The following headers cause gRPC's C++ implementation to abort() when called via http2: te: x (x != trailers) :scheme: x (x != http, https) grpclb_client_stats: x (x == anything) On top of sending one of those headers, a later header must be sent that gets the total header size past 8KB. We recommend upgrading past git commitï¿½2485fa94bd8a723e5c977d55a3ce10b301b437f8 or v1.53 and above.	CVE-2023-1428	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/grpc-protobuf-1.45.1.jar	io.grpc:grpc-protobuf	< 1.53.0	1.53.0	2023-07-18T02:28:09-05:00
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.	CVE-2020-36189	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-36184	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-11113	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-14060	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-35491	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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).	CVE-2020-11112	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes.	CVE-2019-10172	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	<= 1.9.13		2023-07-18T02:26:10-05:00
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).	CVE-2020-10968	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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).	CVE-2020-14195	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-36181	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint, the service has the mysql-connector-java jar (8.0.14 or earlier) in the classpath, and an attacker can host a crafted MySQL server reachable by the victim, an attacker can send a crafted JSON message that allows them to read arbitrary local files on the server. This occurs because of missing com.mysql.cj.jdbc.admin.MiniAdmin validation.	CVE-2019-12086	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
Apache Commons IO Java Deserialization Remote Code Execution		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/commons-io-2.4.jar	commons-io:commons-io	2.4	2.5	2022-11-24T01:25:39-06:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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).	CVE-2020-11619	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-36183	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
Apache Lucene Operations Class Improper Regular Expression Handling CPU Consumption Remote DoS		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/lucene-core-8.7.0.jar	org.apache.lucene:lucene-core	< 8.10.0	8.10.0,9.0.0	2022-04-12T21:26:13-05:00
Javassist main/javassist/bytecode/InstructionPrinter.java InstructionPrinter::instructionString() Function IINC Opcode Handling Unspecified Issue		High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/javassist-3.18.2-GA.jar; sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/javassist-3.18.2-GA.jar/META-INF/maven/org.javassist/javassist/pom.xml	org.javassist:javassist	3.8.0 <= Version <= 3.18.2-GA	3.19.0-GA	2021-11-13T04:47:32-06:00
FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.	CVE-2018-5968	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.1,1.9.13-cloudera.1	2022-11-15T01:26:03-06:00
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.	CVE-2020-36182	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
Elasticsearch Improper API Key Binding Remote Engine Access	CVE-2021-22148	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/elasticsearch-7.10.2.jar	org.elasticsearch:elasticsearch	< 7.14.0	7.14.0	2021-11-13T04:47:32-06:00
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.	CVE-2020-36187	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
In Spring for Apache Kafka 3.0.9 and earlier and versions 2.9.10 and earlier, a possible deserialization attack vector existed, but only if unusual configuration was applied. An attacker would have to construct a malicious serialized object in one of the deserialization exception record headers. Specifically, an application is vulnerable when all of the following are true: * The user does notï¿½configure an ErrorHandlingDeserializer for the key and/or value of the record * The user explicitly sets container properties checkDeserExWhenKeyNull and/or checkDeserExWhenValueNull container properties to true. * The user allows untrusted sources to publish to a Kafka topic By default, these properties are false, and the container only attempts to deserialize the headers if an ErrorHandlingDeserializer is configured. The ErrorHandlingDeserializer prevents the vulnerability by removing any such malicious headers before processing the record.	CVE-2023-34040	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/spring-kafka-2.8.11.jar	org.springframework.kafka:spring-kafka	2.8.0 <= Version < 2.9.11,3.0.0 <= Version < 3.0.10	2.9.11,3.0.10	2023-08-31T02:26:34-05:00
When gRPC HTTP2 stack raised a header size exceeded error, it skipped parsing the rest of the HPACK frame. This caused any HPACK table mutations to also be skipped, resulting in a desynchronization of HPACK tables between sender and receiver. If leveraged, say, between a proxy and a backend, this could lead to requests from the proxy being interpreted as containing headers from different proxy clients - leading to an information leak that can be used for privilege escalation or data exfiltration. We recommend upgrading beyond the commit contained inï¿½ https://github.com/grpc/grpc/pull/33005 https://github.com/grpc/grpc/pull/33005	CVE-2023-32731	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/grpc-protobuf-1.45.1.jar	io.grpc:grpc-protobuf	< 1.53.0	1.53.0	2023-07-18T02:28:29-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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.	CVE-2020-36188	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to javax.swing.JEditorPane.	CVE-2020-10969	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2021-20190	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2020-25649	High	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2022-11-15T01:26:13-06:00
Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `SniHandler` can allocate up to 16MB of heap for each channel during the TLS handshake. When the handler or the channel does not have an idle timeout, it can be used to make a TCP server using the `SniHandler` to allocate 16MB of heap. The `SniHandler` class is a handler that waits for the TLS handshake to configure a `SslHandler` according to the indicated server name by the `ClientHello` record. For this matter it allocates a `ByteBuf` using the value defined in the `ClientHello` record. Normally the value of the packet should be smaller than the handshake packet but there are not checks done here and the way the code is written, it is possible to craft a packet that makes the `SslClientHelloHandler`. This vulnerability has been fixed in version 4.1.94.Final.	CVE-2023-34462	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/netty-handler-4.1.86.Final.jar	io.netty:netty-handler	< 4.1.94.Final	4.1.94.Final	2023-07-18T02:28:09-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
FasterXML jackson-databind 2.x before 2.9.9.1 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.	CVE-2019-12384	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2022-11-15T01:26:06-06:00
Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local information disclosure vulnerability. This is due to the use of the File.createTempFile which creates a file inside of the system temporary directory with the permissions: -rw-r--r--. Thus the contents of this file are viewable by all other users locally on the system. As such, if the contents written is security sensitive, it can be disclosed to other local users.	CVE-2021-28168	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jersey-common-2.30.jar	org.glassfish.jersey.core:jersey-common	2.28 <= Version < 2.34,3.0.0 <= Version < 3.0.2	2.34,3.0.2	2023-07-18T02:26:12-05:00
Apache HttpComponents HttpClient Request URI Parsing Improper Authority Usage Weakness		Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/commons-httpclient-3.1.jar	apache-httpclient:commons-httpclient	3.1		2021-11-13T04:47:37-06:00
gRPC contains a vulnerability whereby a client can cause a termination of connection between a HTTP2 proxy and a gRPC server: a base64 encoding error for `-bin` suffixed headers will result in a disconnection by the gRPC server, but is typically allowed by HTTP2 proxies. We recommend upgrading beyond the commit inï¿½ https://github.com/grpc/grpc/pull/32309 https://www.google.com/url	CVE-2023-32732	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/grpc-protobuf-1.45.1.jar	io.grpc:grpc-protobuf	< 1.53.0	1.53.0	2023-08-04T02:26:03-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote -- even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue.	CVE-2023-26049	Medium	sha256__2dfa86c9ac006769daad6edfb39ecb5c271d201e7a128bb39a6e9d8db1013cd9.tar.gz/jetty-runner.jar/META-INF/maven/org.eclipse.jetty/jetty-server/pom.xml	org.eclipse.jetty:jetty-server	< 9.4.51.v20230217,10.0.0 <= Version < 10.0.14,11.0.0 <= Version < 11.0.14,12.0.0alpha0 <= Version < 12.0.0.beta0	10.0.14,11.0.14,12.0.0.beta0,9.4.51.v20230217	2023-07-18T02:28:09-05:00
Apache Commons CLI Path Subversion Local Privilege Escalation		Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/commons-cli-1.0.jar	commons-cli:commons-cli	<= 1.2	1.3-RC1	2021-11-13T04:47:33-06:00
A memory disclosure vulnerability was identified in Elasticsearch 7.10.0 to 7.13.3 error reporting. A user with the ability to submit arbitrary queries to Elasticsearch could submit a malformed query that would result in an error message returned containing previously used portions of a data buffer. This buffer could contain sensitive information such as Elasticsearch documents or authentication details.	CVE-2021-22145	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/elasticsearch-rest-client-7.10.2.jar	org.elasticsearch.client:elasticsearch-rest-client	7.10.0 <= Version < 7.13.4	7.13.4	2023-07-18T02:27:33-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `SniHandler` can allocate up to 16MB of heap for each channel during the TLS handshake. When the handler or the channel does not have an idle timeout, it can be used to make a TCP server using the `SniHandler` to allocate 16MB of heap. The `SniHandler` class is a handler that waits for the TLS handshake to configure a `SslHandler` according to the indicated server name by the `ClientHello` record. For this matter it allocates a `ByteBuf` using the value defined in the `ClientHello` record. Normally the value of the packet should be smaller than the handshake packet but there are not checks done here and the way the code is written, it is possible to craft a packet that makes the `SslClientHelloHandler`. This vulnerability has been fixed in version 4.1.94.Final.	CVE-2023-34462	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/neo4j-java-driver-4.4.9.jar/META-INF/maven/io.netty/netty-handler/pom.xml	io.netty:netty-handler	< 4.1.94.Final	4.1.94.Final	2023-07-18T02:28:09-05:00
An issue was discovered jackson-databind thru 2.15.2 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	CVE-2023-35116	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-databind-2.15.2.jar	com.fasterxml.jackson.core:jackson-databind	<= 2.15.2		2023-08-25T02:26:05-05:00
In Elasticsearch versions before 7.13.3 and 6.8.17 an uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.	CVE-2021-22144	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/elasticsearch-7.10.2.jar	org.elasticsearch:elasticsearch	< 6.8.17,7.0.0-alpha1 <= Version < 7.13.3	6.8.17,7.13.3	2023-07-18T02:27:33-05:00
Okio GzipSource unhandled exception Denial of Service	CVE-2023-3635	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/okio-jvm-2.8.0.jar	com.squareup.okio:okio	< 3.4.0		2023-07-13T02:26:57-05:00
In JetBrains Kotlin before 1.4.21, a vulnerable Java API was used for temporary file and folder creation. An attacker was able to read data from such files and list directories due to insecure permissions.	CVE-2020-29582	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/kotlin-stdlib-1.4.10.jar	org.jetbrains.kotlin:kotlin-stdlib	< 1.4.21	1.4.21	2023-07-18T02:26:04-05:00
In JetBrains Kotlin before 1.6.0, it was not possible to lock dependencies for Multiplatform Gradle Projects.	CVE-2022-24329	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/kotlin-stdlib-1.4.10.jar	org.jetbrains.kotlin:kotlin-stdlib	< 1.6.0	1.6.0	2023-07-18T02:26:13-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	CVE-2022-21363	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/mysql-connector-java-8.0.20.jar	mysql:mysql-connector-java	< 8.0.28	8.0.28	2023-07-18T02:26:13-05:00
Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Connectors accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:H).	CVE-2021-2471	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/mysql-connector-java-8.0.20.jar	mysql:mysql-connector-java	8.0.0 <= Version < 8.0.27	8.0.27	2023-07-18T02:28:09-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Jetty is a java based web server and servlet engine. In affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call `HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0` which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service -- although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize` which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory).	CVE-2023-26048	Medium	sha256__2dfa86c9ac006769daad6edfb39ecb5c271d201e7a128bb39a6e9d8db1013cd9.tar.gz/jetty-runner.jar/META-INF/maven/org.eclipse.jetty/jetty-server/pom.xml	org.eclipse.jetty:jetty-server	< 9.4.51.v20230217,10.0.0 <= Version < 10.0.14,11.0.0 <= Version < 11.0.14	10.0.14,11.0.14,9.4.51.v20230217	2023-07-18T02:28:09-05:00
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.	CVE-2019-12814	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/jackson-mapper-asl-1.9.13.jar	org.codehaus.jackson:jackson-mapper-asl	1.5.0 <= Version <= 1.9.13	1.8.10-cloudera.3,1.9.13-cloudera.3	2023-04-16T02:26:03-05:00
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.	CVE-2021-29425	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/commons-io-2.4.jar	commons-io:commons-io	< 2.7	2.7	2023-07-18T02:28:09-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
Elasticsearch versions before 7.11.2 and 6.8.15 contain a document disclosure flaw was found in the Elasticsearch suggester and profile API when Document and Field Level Security are enabled. The suggester and profile API are normally disabled for an index when document level security is enabled on the index. Certain queries are able to enable the profiler and suggester which could lead to disclosing the existence of documents and fields the attacker should not be able to view.	CVE-2021-22135	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/elasticsearch-7.10.2.jar	org.elasticsearch:elasticsearch	< 6.8.15,7.0.0 <= Version < 7.11.2	6.8.15,7.11.2	2023-07-18T02:28:09-05:00
A document disclosure flaw was found in Elasticsearch versions after 7.6.0 and before 7.11.0 when Document or Field Level Security is used. Get requests do not properly apply security permissions when executing a query against a recently updated document. This affects documents that have been updated and not yet refreshed in the index. This could result in the search disclosing the existence of documents and fields the attacker should not be able to view.	CVE-2021-22134	Medium	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/elasticsearch-7.10.2.jar	org.elasticsearch:elasticsearch	7.6.0 <= Version < 7.11.0	7.11.0	2023-07-18T02:28:09-05:00
In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario.	CVE-2022-2047	Low	sha256__2dfa86c9ac006769daad6edfb39ecb5c271d201e7a128bb39a6e9d8db1013cd9.tar.gz/jetty-runner.jar/META-INF/maven/org.eclipse.jetty/jetty-http/pom.xml	org.eclipse.jetty:jetty-http	< 9.4.47,10.0.0 <= Version < 10.0.10,11.0.0 <= Version < 11.0.10	10.0.10,11.0.10,9.4.47	2023-07-18T02:28:25-05:00

Summary	CVEs	Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited
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.	CVE-2020-8908	Low	sha256__d7e9bc70748cf4518235e4b35448d7a2da5305c7303227dd291329d45cad843e.tar.gz/datahub/datahub-gms/bin/war.war/WEB-INF/lib/graphql-java-19.5.jar/META-INF/maven/com.google.guava/guava/pom.xml	com.google.guava:guava	< 32.0.0	32.0.0	2023-08-19T02:27:34-05:00