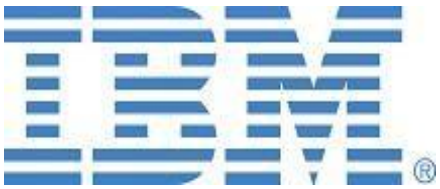

2020

CVEs and Statements of Impact for IBM Spectrum Symphony 7.3.0 and IBM Spectrum Conductor 2.4.1

IBM SPECTRUM SYMPHONY 7.3.0 AND IBM SPECTRUM CONDUCTOR 2.4.1

Contents

Common Vulnerabilities and Exposures (CVEs) and statements of impact for IBM Spectrum Symphony 7.3.0 and IBM Spectrum Conductor 2.4.1

This document lists CVEs for various third-party software included with IBM Spectrum Symphony 7.3.0 or IBM Spectrum Conductor 2.4.1. It also provides the impact, if any, that those CVEs may have to an environment with both products. For cases where there may be impact or potential impact, this document provides suggested mitigation strategies.

The analysis provided is based on the current product usage of IBM Spectrum Symphony 7.3.0 and IBM Spectrum Conductor 2.4.1 and is subject to change as https://cve.mitre.org/ publishes new or updates vulnerabilities.

mesos-1.4.0-shaded-protobuf.jar from Spark 2.3.3 and Spark 2.4.3

- CVE-2018-11793
- CVE-2018-1330
- CVE-2018-8023
- CVE-2019-0204
- CVE-2019-5736

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/mesos-1.4.0-shaded-protobuf.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/mesos-1.4.0-shaded-protobuf.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/mesos-1.4.0-shaded-protobuf.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/mesos-1.4.0-shaded-protobuf.jar

Statement: These five CVEs are related to Apache Mesos. They have no impact to IBM Spectrum Conductor since it does not use Mesos.

Mitigation: If Mesos will be used, he mitigation of these CVEs is dependent on the open source Spark package upgrading to a non-vulnerable version of Mesos.

libthrift-0.9.3.jar from Spark 2.3.3 and Spark 2.4.3

- CVE-2016-5397

Statement: The Spark community is tracking this CVE (https://issues.apache.org/jira/browse/SPARK-24229), and has stated that Spark itself is not vulnerable to the issue since the Apache Thrift Go client library is not used by Spark. Therefore, this CVE does not affect IBM Spectrum Conductor.

- CVE-2018-11798
- CVE-2018-1320
- CVE-2019-0205
- CVE-2019-0210

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/libthrift-0.9.3.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/libthrift-0.9.3.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/libthrift-0.9.3.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/libthrift-0.9.3.jar

Statement: These four CVEs have no impact to IBM Spectrum Conductor since JPMC is not currently using the Thrift node.js static file server.

Mitigation: If Thrift will be use, the mitigation of these CVEs is dependent on the open source Spark package upgrading to a non-vulnerable version of Thrift (v0.12.0 or higher).

libthrift-0.10.0.jar from Spark 2.1.1

- CVE-2018-11798
- CVE-2018-1320
- CVE-2019-0205
- CVE-2019-0210

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/libthrift-0.10.0.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/libthrift-0.10.0.jar

Statement: These four CVEs have no impact to IBM Spectrum Conductor since JPMC is not currently using the Thrift node.js static file server.

Mitigation: If Thrift will be use, the mitigation of these CVEs is dependent on the open source Spark package upgrading to a non-vulnerable version of Thrift (v0.12.0 or higher).

zookeeper-3.4.6.jar from Spark 2.1.1, Spark 2.3.3, and Spark 2.4.3

- CVE-2017-5637
- CVE-2018-8012
- CVE-2019-0201

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/zookeeper-3.4.6.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/zookeeper-3.4.6.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/zookeeper-3.4.6.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/zookeeper-3.4.6.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/zookeeper-3.4.6.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/zookeeper-3.4.6.jar

Statement: These three CVEs have no impact to IBM Spectrum Conductor as it does not use Zookeeper for Spark high availability (HA). IBM Spectrum Conductor has its own implementation.

Mitigation: If Zookeeper will be used, the mitigation of these CVEs is dependent on the open source Spark package upgrading to a non-vulnerable version of Zookeeper (v3.4.13 or higher).

derby-10.12.1.1.jar from Spark 2.1.1, Spark 2.3.3, and Spark 2.4.3

- CVE-2018-1313

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/derby-10.12.1.1.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/derby-10.12.1.1.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/derby-10.12.1.1.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/derby-10.12.1.1.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/derby-10.12.1.1.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/derby-10.12.1.1.jar

Statement: This CVE is only a vulnerability when using a Derby database that either does not use a policy file, or one that uses the default policy file.

Mitigation: If a Derby database is required for Hive or other purposes, configure the database using a Java Security Manager policy file that is configured in such a way that the attack will not work.

icu4j-56_1.jar from /wlp and /gui directories

- CVE-2017-15396
- CVE-2017-15422

Location:
$EGO_TOP/gui/3.8/lib/icu4j-56_1.jar

$EGO_TOP/wlp/usr/servers/gui/apps/perf/3.8/perfgui/WEB-INF/lib/icu4j-56_1.jar

$EGO_TOP/wlp/usr/servers/gui/apps/perf/3.8/perfguiv5/WEB-INF/lib/icu4j-56_1.jar

$EGO_TOP/wlp/usr/servers/gui/apps/soam/7.3/symgui/WEB-INF/lib/icu4j-56_1.jar

$EGO_TOP/wlp/usr/shared/resources/rest/3.8/icu4j-56_1.jar

Statement: These two CVEs are related to stack buffer overflow in the V8 JavaScript engine for the Google Chrome client, affecting Chrome versions prior to version 63.0. 3239.84. These CVEs do not affect IBM Spectrum Symphony 7.3.0 or IBM Spectrum Conductor because those product levels support Google Chrome 77, and the CVEs do not apply to newer versions of Chrome.

Apache log4j-1.2.16.jar from /hostfactory, /is, /gui, /wlp, /perf, and /mapreduce directories

- CVE-2019-17571

Location:
$EGO_TOP/3.8/hostfactory/providers/common/lib/log4j-1.2.16.jar

$EGO_TOP/is/7.3/lib/log4j-1.2.16.jar

$EGO_TOP/gui/3.8/lib/log4j-1.2.16.jar

$EGO_TOP/wlp/usr/shared/resources/rest/3.8/log4j-1.2.16.jar

$EGO_TOP/perf/3.8/lib/log4j-1.2.16.jar

$EGO_TOP/soam/mapreduce/7.3/linux-x86_64/lib/log4j-1.2.16.jar

Statement: This CVE is for the log4j socket server. Both IBM Symphony (7.1.2 and 7.3.0) and IBM Spectrum Conductor are not affected by this issue since they do not use SocketAppender in their configuration files.

Apache log4j-1.2.17.jar from /ascd and /mapreduce directories, and from Spark 2.1.1, Spark 2.3.3, and Spark 2.4.3

- CVE-2019-17571

Location:

$EGO_TOP/ascd/2.4.1/lib/log4j-1.2.17.jar

$EGO_TOP/conductorspark/2.4.1/lib/log4j-1.2.17.jar

$EGO_TOP /conductorspark/conf/packages/Spark2.3.3-Conductor2.4.1/spark-2.3.3-hadoop-2.7/jars/log4j-1.2.17.jar

$EGO_TOP /conductorspark/conf/packages/Spark2.1.1-Conductor2.4.1/spark-2.1.1-hadoop-2.7/jars/log4j-1.2.17.jar

$EGO_TOP /conductorspark/conf/packages/Spark2.4.3-Conductor2.4.1.bak/spark-2.4.3-hadoop-2.7/jars/log4j-1.2.17.jar

$EGO_TOP/soam/mapreduce/7.3/linux-x86_64/lib/hadoop-2.7.x/log4j-1.2.17.jar

Statement: This CVE is for the log4j socket server. Both IBM Symphony (7.1.2 and 7.3.0) and IBM Spectrum Conductor are not affected by this issue since they do not use SocketAppender in their configuration files.

netty-3.8.0.Final.jar from Spark 2.1.1

- CVE-2014-0193
- CVE-2014-3488

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/netty-3.8.0.Final.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/netty-3.8.0.Final.jar

Statement: These two CVEs have no impact to IBM Spectrum Conductor as the Spark community states that Netty 3 is not directly used in Spark (see https://issues.apache.org/jira/browse/SPARK-18586 for details).

Mitigation: If Netty will be used, the mitigation of these CVEs is dependent on the open source Spark package upgrading the version of Netty. When Spark 3.0 is released, it will include Netty v4.1.42.

jackson-databind-2.6.7.1.jar from Spark 2.1.1, Spark 2.3.3, and Spark 2.4.3

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/jackson-databind-2.6.7.1.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/jackson-databind-2.6.7.1.jar

$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/jackson-databind-2.6.7.1.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.1.1-Conductor2.4.1/Spark2.1.1.tgz#/spark-2.1.1-hadoop-2.7.tgz#/spark-2.1.1-hadoop-2.7/jars/jackson-databind-2.6.7.1.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.4.3-Conductor2.4.1/Spark2.4.3.tgz#/spark-2.4.3-hadoop-2.7.tgz#/spark-2.4.3-hadoop-2.7/jars/jackson-databind-2.6.7.1.jar

$EGO_TOP/conductorspark/conf/packages/Spark2.3.3-Conductor2.4.1/Spark2.3.3.tgz#/spark-2.3.3-hadoop-2.7.tgz#/spark-2.3.3-hadoop-2.7/jars/jackson-databind-2.6.7.1.jar

Overall statement for jackson-databind-2.6.7.1: All vulnerabilities found in jackson-databind-2.6.7.1.jar have no impact to the IBM Spectrum Conductor Spark framework and Spark workload. The following sections provide statements to explain why IBM Spectrum Conductor is not vulnerable to the specific CVEs.

- CVE-2017-15095

  Statement: IBM Spectrum Conductor is not affected because the Spark framework does not use objectMapper.enableDefaultTyping(...) to enable unknown object polymorphic deserialization (see https://access.redhat.com/security/cve/CVE-2017-15095 for details).

- CVE-2018-1000873

  Statement: This CVE is related to performance issues (potential denial of service) when deserializing malicious input, specifically including very large numeric values in the nanoseconds field of the time value. IBM Spectrum Conductor does not use the functionality, so there is no impact.

- CVE-2018-11307

Statement: IBM Spectrum Conductor is not affected by this issue since the Spark Java runtime environment does not load MyBatis classes to exploit this vulnerability.

- CVE-2018-14718

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include slf4j-ext.jar.

- CVE-2018-14719

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include or provide the requisite gadget.jar file.

- CVE-2018-14720

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the com.sun.deploy.security.ruleset.DRSHelper class.

- CVE-2018-14721

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the axis2-jaxws.jar file.

- CVE-2018-19360

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the axis2-transport-jms.jar file.

- CVE-2018-19361

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the openjp.jar file.

- CVE-2018-19362

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the jboss-common-core.jar file.

- CVE-2018-5968

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not trigger polymorphic deserialization globally using objectMapper.enableDefaultTyping() to enable unknown object polymorphic deserialization.

- CVE-2018-7489

  Statement: This CVE is related to the readValue method of the ObjectMapper. This does not affect IBM Spectrum Conductor since it uses the readValue method to convert JSON to Object, but it does not support c3p0 classes as polymorphic deserialization for CVE-2018-7489.

- CVE-2019-12086

Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the mysql-connector-java.jar file in the classpath.

- CVE-2019-12384

  Statement: This CVE relies on logback-core (ch.qos.logback.core) being present in the application's ClassPath. IBM Spectrum Conductor is not affected by this issue since it does not include Logback-core and does not use Logback in any supported configuration.

- CVE-2019-12814

  Statement: IBM Spectrum Conductor is not affected by this issue since does not include the jdom.jar or jdom2.jar files.

- CVE-2019-14379

  Statement: IBM Spectrum Conductor is not affected by this issue since it uses SubTypeValidator.java 2.6.7.1 and this issue only exists on newer versions (version 2.7 and later).

- CVE-2019-14439

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the logback jar file.

- CVE-2019-14540

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include Hikari.

- CVE-2019-14892

  Statement: This CVE occurs for polymorphic unmarshmalling. IBM Spectrum Conductor is not affected by this issue since it does not enable polymorphic unmarshmalling. (see https://access.redhat.com/security/cve/cve-2019-14892 for details).

- CVE-2019-14893

  Statement: This CVE occurs for polymorphic unmarshmalling. IBM Spectrum Conductor is not affected by this issue since it does not enable polymorphic unmarshmalling. (see https://access.redhat.com/security/cve/cve-2019-14893 for details).

- CVE-2019-16335

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include Hikari.

- CVE-2019-16942

  Statement: This CVE occurs for polymorphic unmarshmalling. IBM Spectrum Conductor is not affected by this issue since it does not enable polymorphic unmarshmalling.

- CVE-2019-16943

  Statement: This CVE occurs for polymorphic unmarshmalling. IBM Spectrum Conductor is not affected by this issue since it does not enable polymorphic unmarshmalling, and it does not include the p6spy.jar file.

- CVE-2019-17267

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the ehcache.jar file.

- CVE-2019-20330

  Statement: IBM Spectrum Conductor is not affected by this issue since it does not include the ehcache.jar file.

- CVE-2020-8840

  Statement: This CVE is related to xbean-reflect and JNDI blocking. FasterXML jackson-databind version 2.0.0 through 2.9.10.2 lack certain xbean-reflect and JNDI blocking (as demonstrated by org.apache.xbean.propertyeditor.JndiConverter). IBM Spectrum Conductor does not use xbean-reflect or JNDI.

Overall mitigation for jackson-databind-2.6.7.1: The mitigation of these CVEs is dependent on the open source Spark package upgrading the version of Jackson-databind. When Spark 3.0 is released, it will include Jackson-databind to version 2.10.0.

jackson-databind-2.8.11.3.jar from Elasticsearch 7.2.1

Location:
$EGO_TOP/integration/elk/1.4.3/elasticsearch-7.2.1/plugins/search-guard-7/jackson-databind-2.8.11.3.jar

$EGO_TOP/integration/elk/1.4.3/elasticsearch-7.2.1/modules/ingest-geoip/jackson-databind-2.8.11.3.jar

Overall statement for jackson-databind-2.8.11.3: Other than CVE 2018-1000873, all other CVEs found in jackson-databind-2.8.11.3.jar have no impact to IBM Spectrum Conductor. The following sections provide statements to explain the impact of the CVEs to IBM Spectrum Conductor.

- CVE-2018-1000873

  Statement: This vulnerability is related to performance issues (potential denial of service) when deserializing malicious input, specifically including very large numeric values in the nanoseconds field of the time value. There is no fix for this CVE in the Jackson-databind 2.8.x stream.

  The Elasticsearch community has stated that the Logstash ingest-geoip module is not vulnerable to this CVE, because it only serializes and deserializes objects which are internally created and controlled.

There is no statement about vulnerability status within the Search Guard community. If vulnerable, the potential impact of this vulnerability is denial of service in the authentication layer of the Elastic Stack. In this case, all Spark application would continue to run, but some metrics (for example resource usage charts) would not be available.

Mitigation: The Search Guard component will be removed entirely in the next version of IBM Spectrum Conductor.

- CVE-2018-14719

  Statement: IBM Spectrum Conductor is not affected by this issue since this vulnerability was fixed in jackson-databind-2.8.11.3 (see to https://github.com/advisories/GHSA-4gq5-ch57-c2mg for details).

- CVE-2018-14720

  Statement: IBM Spectrum Conductor is not affected by this issue since this vulnerability was fixed in jackson-databind-2.8.11.3 (see https://github.com/advisories/GHSA-x2w5-5m2g-7h5m for details).

- CVE-2018-14721

  Statement: IBM Spectrum Conductor is not affected by this issue since this vulnerability was fixed in jackson-databind-2.8.11.3 (see https://github/advisories/GHSA-9mxf-g3x6-wv74 for details).

- CVE-2018-19360

  Statement: IBM Spectrum Conductor is not affected by this issue since this vulnerability was fixed in jackson-databind-2.8.11.3 (see https://github.com/advisories/GHSA-f9hv-mg5h-xcw9 for details).

- CVE-2018-19361
  Statement: IBM Spectrum Conductor is not affected by this issue since this vulnerability was fixed in jackson-databind-2.8.11.3 (see https://github.com/advisories/GHSA-mx9v-gmh4-mgqw for details).

- CVE-2018-19362

  Statement: IBM Spectrum Conductor is not affected by this issue since this vulnerability was fixed in jackson-databind-2.8.11.3 (see https://github.com/advisories/GHSA-c8hm-7hpq-7jhg for details).

- CVE-2019-12086

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the mysql-connector-java.jar file.

- CVE-2019-12384

Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the logback-core.jar file.

- CVE-2019-12814

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the jdom.jar file.

- CVE-2019-14379

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the ehcache.jar file.

- CVE-2019-14439

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the logback.jar file.

- CVE-2019-14540

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the hikari.jar file.

- CVE-2019-14892

  Statement: The Search Guard community has indicated that Search Guard is not affected by this vulnerability because it does not enable polymorphic handling in Jackson, which is required for the vulnerability. Furthermore, it only processes trusted data with Jackson. Therefore, IBM Spectrum Conductor, which includes Search Guard, is not vulnerable (see https://forum.search-guard.com/t/jackson-databind-2653-vulnerability/1782/2 for details).

- CVE-2019-14893

  Statement: The Search Guard community has indicated that Search Guard is not affected by this vulnerability because it does not enable polymorphic handling in Jackson, which is required for the vulnerability. Furthermore, it only processes trusted data with Jackson. Therefore, IBM Spectrum Conductor, which includes Search Guard, is not vulnerable (see https://forum.search-guard.com/t/jackson-databind-2653-vulnerability/1782/2 for details).

- CVE-2019-16335

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the hikari.jar file.

- CVE-2019-16942

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the commons-dhcp.jar file.

- CVE-2019-16943

Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the p6spy.jar file.

- CVE-2019-17267

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the ehcach.jar file.

- CVE-2019-20330

  Statement: IBM Spectrum Conductor is not affected by this issue since Elasticsearch services (search-guard and ingest-geoip) do not include the ehcache.jar file.

- CVE-2020-8840

  Statement: IBM Spectrum Conductor is not affected by this issue since the Elasticsearch services (search-guard and ingest-geoip) do not include the xbean-reflect.jar file.

Overall mitigation for jackson-databind-2.8.11.3: The mitigation of these CVEs is dependent on the open source ingest-geoip module upgrading to a non-vulnerable version of Jackson-databind. The version included in Logstash v7.6 contains Jackson-databind 2.8.11.4.jar. This version will be included in the next release of IBM Spectrum Conductor. The search guard component will be completely removed in the next version of IBM Spectrum Conductor.

Jackson-databind-2.9.7.jar from Logstash 7.2.1

Location:

$EGO_TOP/integration/elk/1.4.3/logstash-7.2.1/vendor/bundle/jruby/2.5.0/gems/jrjackson-0.4.8-java/lib/com/fasterxml/jackson/core/jackson-databind/2.9.7/jackson-databind-2.9.7.jar

$EGO_TOP/integration/elk/1.4.3/logstash-7.2.1/vendor/bundle/jruby/2.5.0/gems/logstash-input-beats-6.0.0-java/vendor/jar-dependencies/com/fasterxml/jackson/core/jackson-databind/2.9.7/jackson-databind-2.9.7.jar

Overall statement for jackson-databind-2.9.7: All CVEs found in jackson-databind-2.9.7.jar have no impact to IBM Spectrum Conductor. The following sections provide statements to explain why IBM Spectrum Conductor is not vulnerable to the specific CVEs.

- CVE-2018-1000873

  Statement: The Elasticsearch community has indicated that Logstash is not vulnerable to these types of CVEs since it only uses jackson-databind to serialize and deserialize objects which are created and controlled internally by the Logstash code. Therefore, IBM Spectrum Conductor, which includes Logstash, is not vulnerable.

- CVE-2018-19360

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the axis2-transport-jms.jar file.

- CVE-2018-19361

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the openjpa.jar file.

- CVE-2018-19362

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the jboss-common-core.jar file.

- CVE-2019-12086

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with mysql-connector-java.jar file.

- CVE-2019-12384

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the logback-core.jar file.

- CVE-2019-12814

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the jdom.jar file.

- CVE-2019-14379

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats not included with the ehcache.jar file.

- CVE-2019-14439

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the logback.jar file.

- CVE-2019-14540

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the hikari.jar file.

- CVE-2019-14892

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with commons-configuration.jar or commons-configuration2.jar file.

- CVE-2019-14893

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with xalan.jar file.

- CVE-2019-16335

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the hikari.jar file.

- CVE-2019-16942

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the commons-dhcp.jar file.

- CVE-2019-16943

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the p6spy.jar file.

- CVE-2019-17267

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the ehcache.jar file.

- CVE-2019-20330

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats not include the ehcache.jar file.

- CVE-2020-8840

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-input-beats is not included with the xbean-reflect.jar file.

Overall mitigation for jackson-databind-2.9.7: The mitigation of these CVEs is dependent on the open source logstash-input-beats upgrading to a non-vulnerable version of Jackson-databind. The logstash-input-beats v6.0.4 included in Logstash 7.6 contains Jackson-databind 2.9.10.1. This version will be included in the next release of IBM Spectrum Conductor.

Jackson-databind-2.9.8.jar from Logstash 7.2.1

Location:
$EGO_TOP/integration/elk/1.4.3/logstash-7.2.1/logstash-core/lib/jars/jackson-databind-2.9.8.jar

Overall statement for jackson-databind-2.9.8: All CVEs found in the jackson-databind-2.9.8.jar have no impact to IBM Spectrum Conductor. The following sections provide statements to explain why IBM Spectrum Conductor is not vulnerable to the specific CVEs.

- CVE-2019-12086

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the mysql-connector-java.jar file.

- CVE-2019-12384

Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the logback-core.jar file.

- CVE-2019-12814

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the jdom.jar file.

- CVE-2019-14379

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the ehcache.jar file.

- CVE-2019-14439

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the logback.jar file.

- CVE-2019-14540

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the hikari.jar file.

- CVE-2019-14892

  Statement: The Elasticsearch community has indicated that Logstash is not vulnerable to these types of CVEs since it only uses jackson-databind to serialize and deserialize objects which are created and controlled internally by the Logstash code. Therefore, IBM Spectrum Conductor, which includes Logstash, is not vulnerable (see https://discuss.elastic.co/t/logstash-how-to-solve-the-problem-about-jackson-databind-cve-2019-12384/194134/2 for details).

- CVE-2019-14893

  Statement: The Elasticsearch community has indicated that Logstash is not vulnerable to these types of CVEs since it only uses jackson-databind to serialize and deserialize objects which are created and controlled internally by the Logstash code. Therefore, IBM Spectrum Conductor, which includes Logstash, is not vulnerable (see https://discuss.elastic.co/t/logstash-how-to-solve-the-problem-about-jackson-databind-cve-2019-12384/194134/2 for details).

- CVE-2019-16335

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the hikari.jar file.

- CVE-2019-16942

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the commons-dhcp.jar file.

- CVE-2019-16943

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the p6spy.jar file.

- CVE-2019-17267

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the ehcach.jar file.

- CVE-2019-20330

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the ehcache.jar file.

- CVE-2020-8840

  Statement: IBM Spectrum Conductor is not affected by this issue since logstash-core is not included with the xbean-reflect.jar file.

Overall mitigation for jackson-databind-2.9.8: The mitigation of these CVEs is dependent on the open source logstash-core component upgrading to a non-vulnerable version of Jackson-databind. The logstash-core version 7.6 contains Jackson-databind 2.9.10.1. This version will be included in the next release of IBM Spectrum Conductor.

pct_warnings.py from jupyter_enterprise_gateway-0.9.4 > pycrypto-2.6.1

Location:
$EGO_TOP/conductorspark/activation/conductorsparkcore2.4.1/conf/notebooks/Jupyter-5.4.0/Jupyter-5.4.0.tar.gz#/package/jupyter_enterprise_gateway-0.9.4.tar.gz#/jupyter_enterprise_gateway-0.9.4/pycrypto-2.6.1.tar.gz#/pycrypto-2.6.1/lib/Crypto/pct_warnings.py

$EGO_TOP/conductorspark/conf/notebooks/Jupyter-5.4.0/Jupyter-5.4.0.tar.gz#/package/jupyter_enterprise_gateway-0.9.4.tar.gz#/jupyter_enterprise_gateway-0.9.4/pycrypto-2.6.1.tar.gz#/pycrypto-2.6.1/lib/Crypto/pct_warnings.py

- CVE-2013-7459

Statement: This CVE does not impact IBM Spectrum Conductor when notebook SSL is enabled (SSL is enabled by default). When SSL is enabled for IBM Spectrum Conductor notebooks, JEG uses our SSL certificates, so an external intruder would not be able to connect to JEG and exploit the vulnerability in pycrypto.

Mitigation: In the case that SSL has been disabled, set notebook SSL certificates for tier 3 following these steps:
https://www.ibm.com/support/knowledgecenter/en/SSZU2E_2.4.1/managing_cluster/ssl_sig_setup3_dev.html

- CVE-2018-6594

Statement: This CVE does not impact IBM Spectrum Conductor because it is not applied to jupyter_enterprise_gateway; it is vulnerability for the ElGamal key parameter while jupyter_enterprise_gateway uses only AES encryption.

tokens.py from conductorspark > yaml

Location:
$EGO_TOP/conductorspark/2.4.1/etc/lib3/yaml/tokens.py

$EGO_TOP/conductorspark/2.4.1/etc/lib/yaml/tokens.py

- CVE-2020-1747

Statement: This CVE does not impact IBM Spectrum Conductor since the pyyaml does not include the full_load method or the FullLoader loader.

Copyright and trademark information