Apache Log4j2 Vulnerabilities

Qlik Catalog

Apache Log4j2 Vulnerabilities

This document describes how customers may address vulnerabilities CVE-2021-44228 and CVE-2021-45046, both issues with Apache Log4j2, the third-party logging framework used by Qlik Catalog.

Background

Qlik Catalog uses Apache Log4j2 as its logging framework. On December 10, 2021, vulnerability CVE-2021-44228 was published. On December 14, 2021, vulnerability CVE-2021-45046 was published. Any product using an Apache Log4j2 version prior to 2.16.0 is vulnerable.

Please see the following for more info:

- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://nvd.nist.gov/vuln/detail/CVE-2021-45046
- https://logging.apache.org/log4j/2.x/security.html

Exposure

From May 2021 through November 2021 SR1, the **single-node** releases of Catalog used a vulnerable version of Log4j2 (versions 2.13.2 or 2.15.0).

Depending on both the Catalog version and the cluster deployment, **multi-node** Catalog may use either Log4j 1.x (not vulnerable) or the version of Log4j present on the Hadoop classpath (which may be either Log4j 1.x or 2.x). The Hadoop classpath is composed of the Hadoop libraries supplied by the customer's Hadoop vendor (e.g., AWS EMR, Cloudera CDH/CDP, etc.). Log4j2 may be present on the customer-deployed-and-configured Hadoop classpath, which is not defined or managed by Catalog.

Recommendations

There are separate recommendations for the single- and multi-node versions of the product.

Single-Node: Patch Existing Release

A patch for single-node installations May 2021 through November 2021 SR1 is available, QDC-1285-QlikCatalog-log4j2-patch.zip. Applying this patch to a multi-node installation will have **no** effect as multi-node Catalog does not include Log4j2.

To deploy the patch, do the following (as the service account used to run Catalog, typically 'qdc'):

- `unzip QDC-1285-QlikCatalog-log4j2-patch.zip`
- `execute ./applyHotfix.sh`
- enter the full path to the qdc webapp WEB-INF/lib directory (e.g., /usr/local/qdc/apache-tomcat-9.0.50/webapps/qdc/WEB-INF/lib)
- restart Tomcat

The following is sample output:

```
$ ./applyHotfix.sh
Please input the path to the Catalog webapp WEB-INF/lib folder: /usr/local/qdc/apache-tomcat-
9.0.45/webapps/qdc/WEB-INF/lib

Backup at /home/qdc/log4j2-2021-12-15-11-19-50

BEFORE
-rw-r--r--. 1 qdc qdc  201684 Jan 25  2021 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-1.2-api-2.13.2.jar
-rw-r--r--. 1 qdc qdc  292301 Jan 25  2021 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-api-2.13.2.jar
-rw-r--r--. 1 qdc qdc 1714150 Jan 25  2021 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-core-2.13.2.jar
-rw-r--r--. 1 qdc qdc   23591 Jan 25  2021 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-slf4j-impl-2.13.2.jar
-rw-r--r--. 1 qdc qdc   32723 Jan 25  2021 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-web-2.13.2.jar

Count of jar files:
298

+ rm /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-INF/lib/log4j-1.2-api-2.13.2.jar
+ rm /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-INF/lib/log4j-api-2.13.2.jar
+ rm /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-INF/lib/log4j-core-2.13.2.jar
+ rm /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-INF/lib/log4j-slf4j-impl-2.13.2.jar
+ rm /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-INF/lib/log4j-web-2.13.2.jar
+ cp newjars/log4j-1.2-api-2.16.0.jar newjars/log4j-api-2.16.0.jar newjars/log4j-core-2.16.0.jar
newjars/log4j-slf4j-impl-2.16.0.jar newjars/log4j-web-2.16.0.jar /usr/local/qdc/apache-tomcat-
9.0.45/webapps/qdc/WEB-INF/lib/
+ set +x
The hotfix has been applied

AFTER
-rw-r--r--. 1 qdc qdc  207909 Dec 15 11:19 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-1.2-api-2.16.0.jar
-rw-r--r--. 1 qdc qdc  301892 Dec 15 11:19 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-api-2.16.0.jar
-rw-r--r--. 1 qdc qdc 1789565 Dec 15 11:19 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-core-2.16.0.jar
-rw-r--r--. 1 qdc qdc   24258 Dec 15 11:19 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-slf4j-impl-2.16.0.jar
-rw-r--r--. 1 qdc qdc   35359 Dec 15 11:19 /usr/local/qdc/apache-tomcat-9.0.45/webapps/qdc/WEB-
INF/lib/log4j-web-2.16.0.jar

Count of jar files:
298
```

Multi-Node: It Is Complicated

Multi-node Catalog is deployed on an edge-node built using the Hadoop libraries supplied by the customer's Hadoop vendor (e.g., AWS EMR, Cloudera CDH/CDP, etc.). Log4j2 may be present on the resulting Hadoop classpath and inadvertently picked up by Catalog. The potential presence of Log4j2 on the edge-node is dependent on several factors, including: (1) the cluster vendor; (2) the cluster version used to build the edge node; (3) which Hadoop packages were deployed; and (4) the configuration of the classpath.

To definitively know if multi-node Catalog is at risk, a test for the vulnerability must be explicitly executed. Please contact support to discuss running this test.

If a test cannot be run, there are two options: (1) perform a brute-force search-and-replace for the problematic Log4j2 libraries (see https://www.lunasec.io/docs/blog/log4j-zero-day-mitigation-guide/#manually-scanning-your-dependencies); or (2) put in place the partial mitigation described below.

The below configuration mitigation only partially addresses the two vulnerabilities. It can be used in situations where the edge node cannot be rebuilt or modified.

The following two configuration changes disable the vulnerable expression evaluation feature of Log4j2.

(1) add line to end of Tomcat file bin/setenv.sh:

```
export JAVA_OPTS="$JAVA_OPTS -Dlog4j2.formatMsgNoLookups=true"
```

(2) find and edit property in core_env.properties:

```
# Pipe (|) delimited list of additional arguments to be passed to the Java runtime.

# Default: none

external.job.runner.extra.java.arguments=-Dlog4j2.formatMsgNoLookups=true
```

Restart Tomcat.

Derived from https://www.lunasec.io/docs/blog/log4j-zero-day-mitigation-guide/

About Qlik

Qlik is on a mission to create a data-literate world, where everyone can use data to solve their most challenging problems. Only Qlik's end-to-end data management and analytics platform brings together all of an organization's data from any source, enabling people at any skill level to use their curiosity to uncover new insights. Companies use Qlik to see more deeply into customer behavior, reinvent business processes, discover new revenue streams, and balance risk and reward. Qlik does business in more than 100 countries and serves over 48,000 customers around the world.

qlik.com