DELMIA Quintiq investigation into CVE-2021-44228 Apache Log4j 2

Background

On December 9 2021 a security vulnerability was identified in the Apache Log4j 2 libraries. This vulnerability (as described in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 can lead to remote execution if an attacker can influence the content of messages logged through the log4j library.

Quintiq software versions affected.

Quintiq 4.x – 5.1 → Uses log4j 1.x, which is not impacted

Quintiq 5.2 – 5.4 → Uses log4j version 2.2, which is impacted

Quintiq 5.4 – 6.x → uses log4J version 2.6, which is impacted

The affected parts of the Quintiq software are:

Server side

QIntegrator – Integration tool consuming messages from external parties

QGateway – internet facing communication management tool

QJava Server – component used for BIRT reporting and serverside rendering of gauges

RServer – component used for running R based programs

Client side

QThinClient – front end UI for all Quintiq users

Tooling

The tools are used during configuration and development. Affected tools are:

Configuration Utility – used to configure the Quintiq components,

Log file viewer – used to view log files

Log File Analyzer – used to analyze log files

Diagnostic Report Tool – used to collect logfiles for analysis

System Health Checker – used to send reports from LFA and DRT to sysadmins

BIRT Designer – used to create report templates.

Impact

The impact on the different components is dependent on the attack surface that is given by each of these components and therefore differs per component. Most affected are the server side components that have an open connection to the internet, being the QIntegrator and the QGateway.

Client side components and tooling are less vulnerable as they are not running open communication to the external world, they only communicate to other Quintiq services.

Mitigations

Summary

In order to prevent abuse of the vulnerability there are a number of opportunities. They need to be performed by system administrators of the DELMIA Quintiq systems. For DELMIA Hosted Solutions this is managed by DELMIA Quintiq.

- Zero code change mitigation: The vulnerability can be mitigated by firewall settings.
- Self patching mitigation: The vulnerability can be removed by deleting a problematic class file.
- Hot fix from DELMIA Quintiq: Hotfixes will be released for the affected software versions.

Zero code change mitigation

By using a firewall that blocks outgoing traffic for components that do not need to initiate outgoing traffic to the internet (e.g QGateway) it is possible to guard these processes fully. This is true for QGateway, QJavaServer, QRServer. The QIntegrator is more difficult to protect, but could also be restricted to the intended target hosts.

Self-patching

The vulnerability can be removed by deleting a problematic class file. This fix can be performed on the Quintiq installation.

Quintiq version 6.0 and higher

Using the recommended procedure as described in the CVE, it is possible to remove the offending code from the Quintiq installations by running the following command inside the bin\lib folder of your Quintiq installation.

- zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

Earlier Quintiq versions:

The same procedure is applicable but now the command has to be executed additionally for QLogFileAnalyzer.jar, QLogFileViewer.jar, QDiagnosticReport.jar and QSystemHealthChecker.jar.
For simplicity, the command can also be run for all jar files in the java folder:

- for %f in (*.jar) do zip -q -d %f org/apache/logging/log4j/core/lookup/JndiLookup.class

QThinClient running via JNLP/QJLauncher

Notice that this procedure does not patch the QThinClient when it is run via JNLP or QJLauncher. Both launch protocols require the jar files to be signed, which can only be done by R&D. In order to use this procedure it is needed to use the .exe version of the Quintiq thin client

Patches from DS DELMIA Quintiq

Currently we are working on a patch timeline in which we will bring all actively supported versions of Quintiq that are based on JAVA 8 or higher to log4j version 2.15. For older versions of Quintiq we will create a patched version of log4j 2.6 that no longer has the bug.

These patches will be based on the *latest* patch of the line that has been released until now, so all major minor versions will get a patch on their latest patch. For example, we will release a hotfix for version 6.0.10, but not for version 6.0.9.

Versions in active maintenance will be the first to receive this patch. Patches will be made available through the normal channels.

For any questions please contact DELMIA Quintiq Support as usual (see https://www.3ds.com/support/contact/call-us/submit-a-request/).