Apache Log4j - CVE-2021-44228

This page will be updated over the coming days as and when new information is available.

Introduction

A zero-day vulnerability has been detected in **Apache Log4j** (the java based logging utility) - see **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228** for more detailed information. Any Java application that makes use of Apache Log4j version **2.0 - 2.14.1** is impacted by this vulnerability. Apache has fixed the vulnerability in **Apache Log4j 2.15.0**.

CAST makes use of **Apache Log4j 2.0 - 2.14.1** in various products, therefore this page explains:

- which products are affected by this vulnerability
- how CAST plans to mitigate the threat
- what you can do to prevent the vulnerability from being exploited

Which CAST products are affected by CVE-2021-44228?

CAST Dashboards/RestAPI	All releases of any of the following: • CAST Engineering Dashboard standalone • CAST Health Dashboard standalone • CAST Engineering Dashboard/Health Dashboard combined • CAST RestAPI standalone • CAST Integrated RestAPI for dashboards embedded in AIP Console 1.x • CAST Security Dashboard standalone
CAST AIP Console	All releases of any of the following: • AIP Console front-end service • AIP Node back-end service • CAST Integrated RestAPI for dashboards embedded in AIP Console 1.x
CAST Imaging	All releases since **2.2.0-beta1**. The vulnerability is found in the third-party software **Neo4j 4.2.**

How does CAST plan to mitigate the threat?

CAST will release updates to affected products in the coming days - these updates will contain **Apache Log4j 2.15.0**, which includes the fix for this vulnerability. Only the most recent releases of each affected product will be patched, therefore this necessarily means upgrading to the newest release to receive the patch (CAST highly recommends this in all situations where possible).

Current status:

Affected product	Release containing Apache Log4j 2.15.0	Notes
CAST Dashboards /RestAPI	2.4.1-funcrel	Released **14 Dec 2021**. • https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard&version=2.4.1-funcrel • https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.health&version=2.4.1-funcrel • https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.engineering&version=2.4.1-funcrel • https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.security&version=2.4.1-funcrel • https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.restapi&version=2.4.1-funcrel
	1.28.4-funcrel	
CAST AIP Console	1.26.1-funcrel	Released **14 Dec 2021**. Includes v. 2.4.1-funcrel release of the CAST Integrated RestAPI which includes the fix. • https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.console&version=1.26.1-funcrel
CAST Imaging		

What you can do to prevent the vulnerability from being exploited

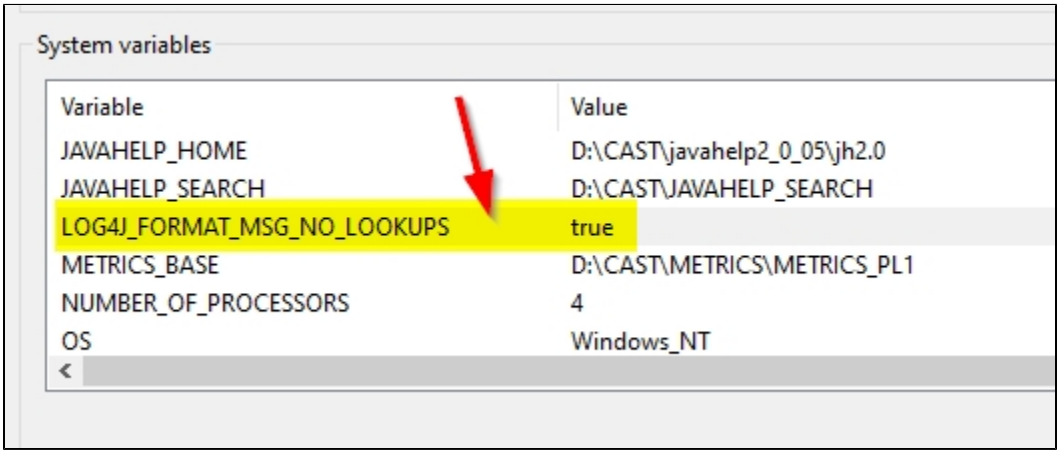
If you are waiting for a patch from CAST for an impacted product, or you cannot upgrade to the CAST product release containing **Apache Log4j 2.15.0**, you can perform the actions listed below to mitigate the vulnerability.

CAST Dashboards/RestAPI

2.0.0-funcrel

Microsoft Windows (WAR or ZIP)

Add a new Microsoft Windows system environment variable as follows: **LOG4J_FORMAT_MSG_NO_LOOKUPS = true** to all servers running a CAST Dashboard/RestAPI either via a WAR or a ZIP file:



Restart Apache Tomcat or the standalone ZIP to ensure the changes are taken into account.

Linux (ZIP)

Edit the following file

```
<unpacked_ZIP>/startup.sh
```

Find the following line:

```
JAVA_OPTS="-Xmx1024m -Xms256m"
```

Update this line to add in `-Dlog4j2.formatMsgNoLookups=true`:

```
JAVA_OPTS="-Xmx1024m -Xms256m -Dlog4j2.formatMsgNoLookups=true"
```

Restart the standalone ZIP to ensure the change is taken into account.

Linux (WAR)

Create a new file called **setenv.sh** in the **CATALINA_BASE/bin** folder:

```
touch setenv.sh
```

Edit this file and add the following line:

```
CATALINA_OPTS=-Dlog4j2.formatMsgNoLookups=true
```

Restart Apache Tomcat or the standalone ZIP to ensure the changes are taken into account.

Any 1.x.x-funcrel release

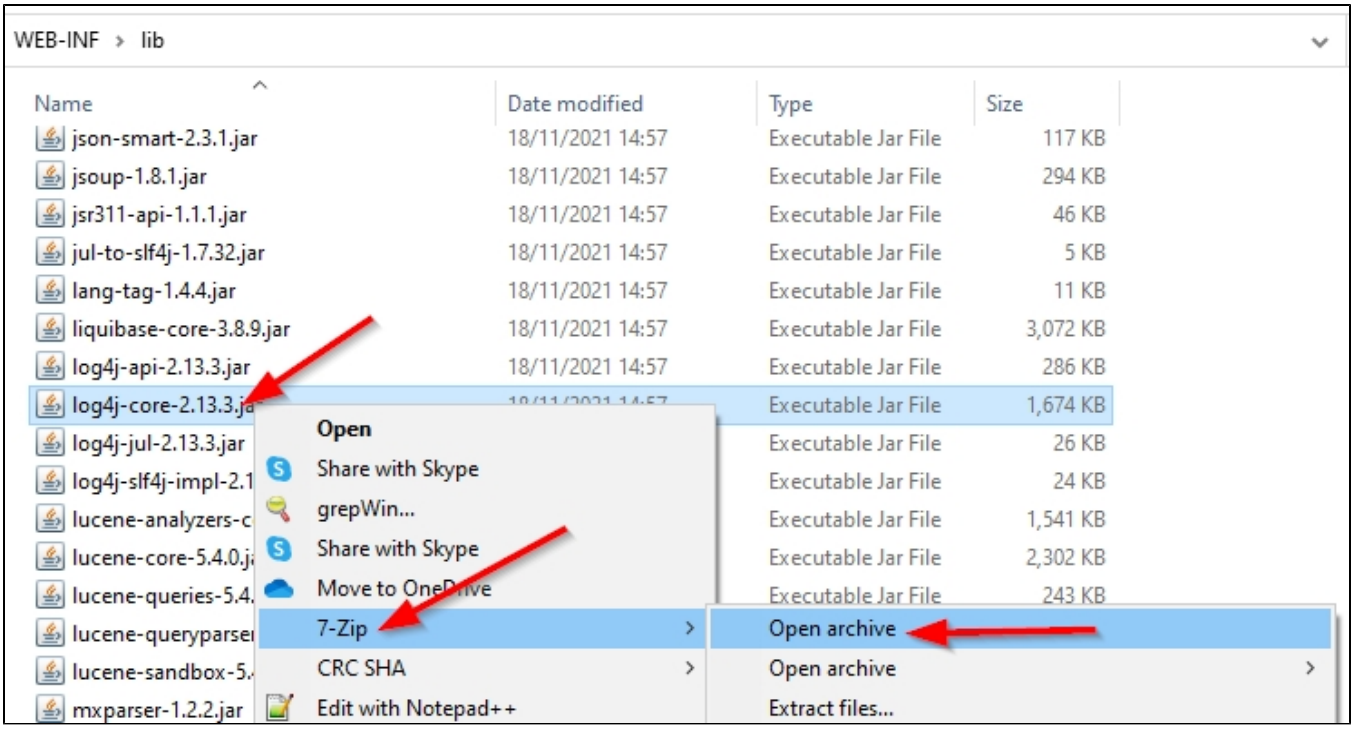
These are older releases of CAST Dashboards/RestAPI and consequently use older releases of **Apache Log4j**. CAST highly recommends upgrading to a newer release anyway, however, if you are still using any of these releases, the mitigation involves **removing a .class** file from a compiled .JAR file. Before starting, please ensure that you **stop** any running services.

Microsoft Windows

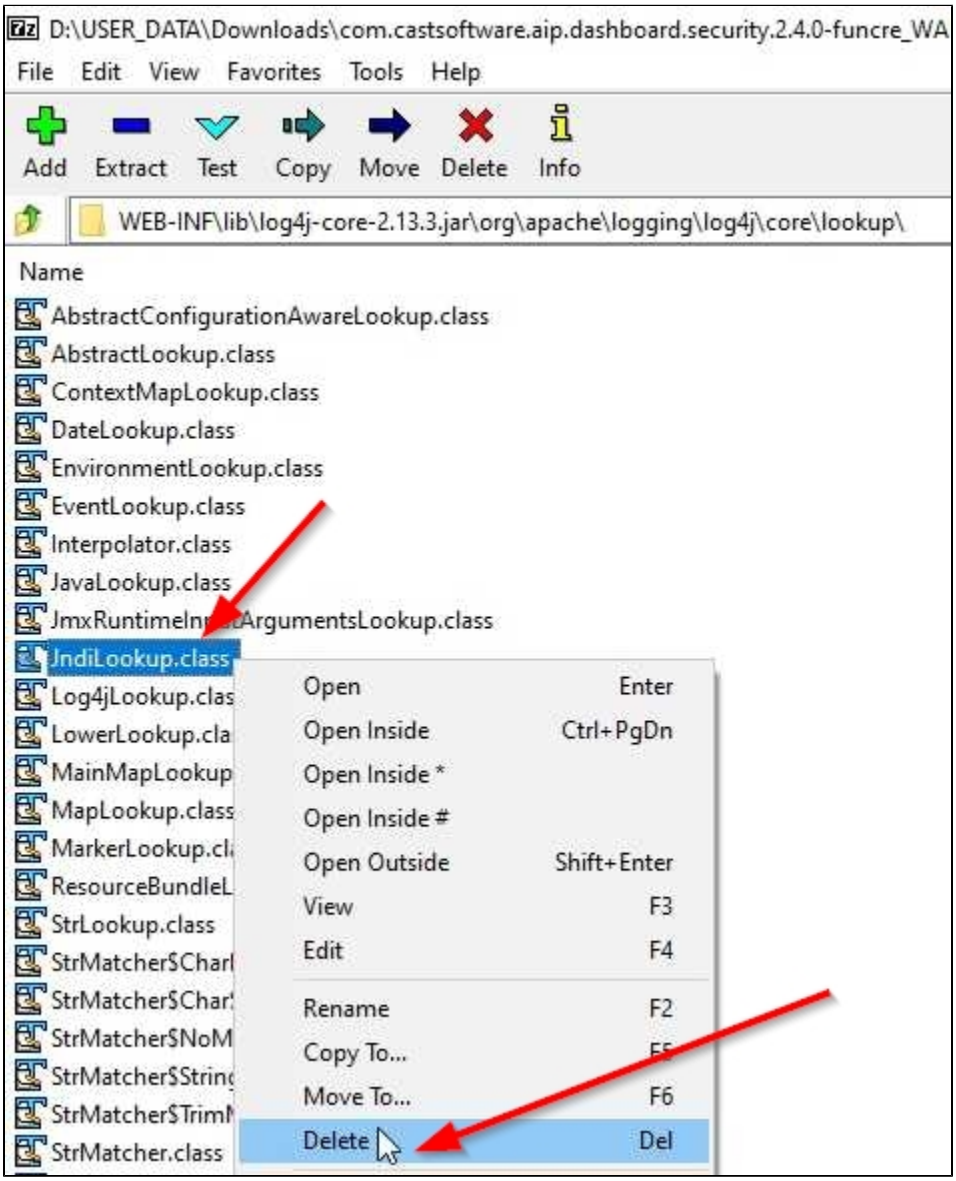
Locate the following file:

```
CATALINA_HOME\webapps\<dashboard>\WEB-INF\lib\log4j-core-*.jar
```

Open the .JAR file with **7Zip** (use the right click **Open Archive** option):



Drill down to the following location: **org\apache\logging\log4j\core\lookup** and locate the **JndiLookup.class** file and then **Delete** this file using the right click menu option:



Now close the 7Zip window. 7Zip will automatically recompile the **log4j-core-*.jar** file. Finally restart Apache Tomcat to ensure that the changes are taken into account.

Linux

Locate the following file:

```
CATALINA_HOME\webapps\<dashboard>\WEB-INF\lib\log4j-core-*.jar
```

Now run the following command to remove a .class file from a the Log4j core JAR file:

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

Finally restart Apache Tomcat to ensure that the changes are taken into account.

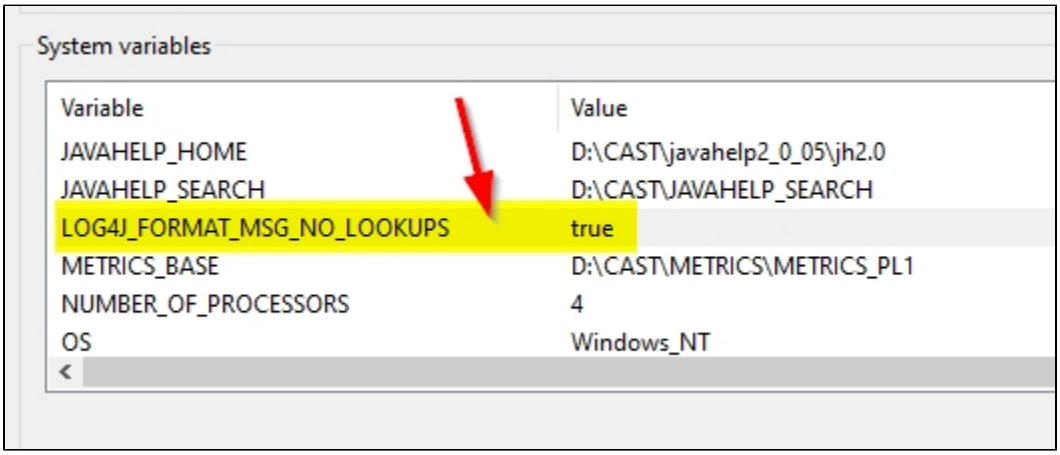
CAST AIP Console

1.10.0-funcrel

These releases include Apache Log4j **2.10** and **2.14.1**.

Microsoft Windows

Add a new Microsoft Windows system environment variable as follows: **LOG4J_FORMAT_MSG_NO_LOOKUPS = true** to all servers running either **AIP Console service** or the **AIP Node service**:



Restart both the AIP Console service and all AIP Node services to ensure the change is taken into account.

Linux (AIP Console service only)

Edit the following file

```
$HOME/CAST/AIPConsole/tools/runAIPConsole.sh
```

Find the following line:

```
JAVA_OPTS="-Xmx1024m -Xms256m"
```

Update this line to add in `-Dlog4j2.formatMsgNoLookups=true`:

```
JAVA_OPTS="-Xmx1024m -Xms256m -Dlog4j2.formatMsgNoLookups=true"
```

Restart the AIP Console service to ensure the change is taken into account.

1.9.0-funcrel

These are very old releases of AIP Console and use **Apache Log4j 2.7**, therefore CAST highly recommends upgrading to a newer release anyway, however, if you are still using any of these releases, the mitigation involves **removing a .class** file from a compiled .JAR file for both the AIP Console service and all AIP Node services. Before starting, please ensure that you **stop** any running services.

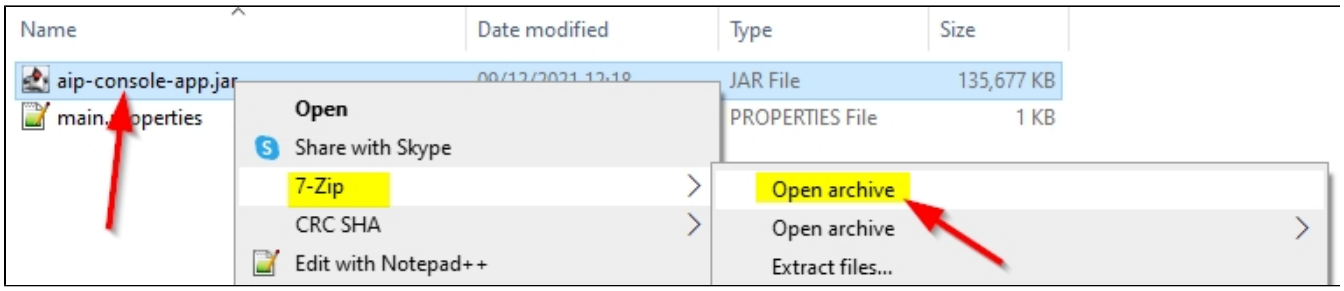
Microsoft Windows

Locate the following files and repeat the instructions below for all files:

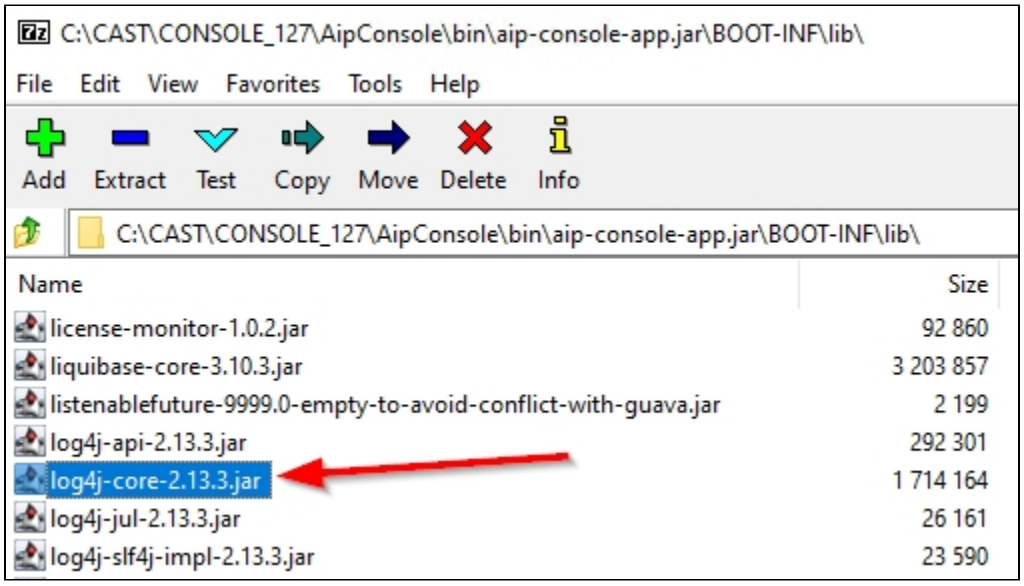
```
AIP Console front-end service
%PROGRAMFILES%\CAST\AipConsole\bin\aip-console-app.jar

All AIP Node services
%PROGRAMFILES%\CAST\AipConsole\bin\aip-node-app.jar
```

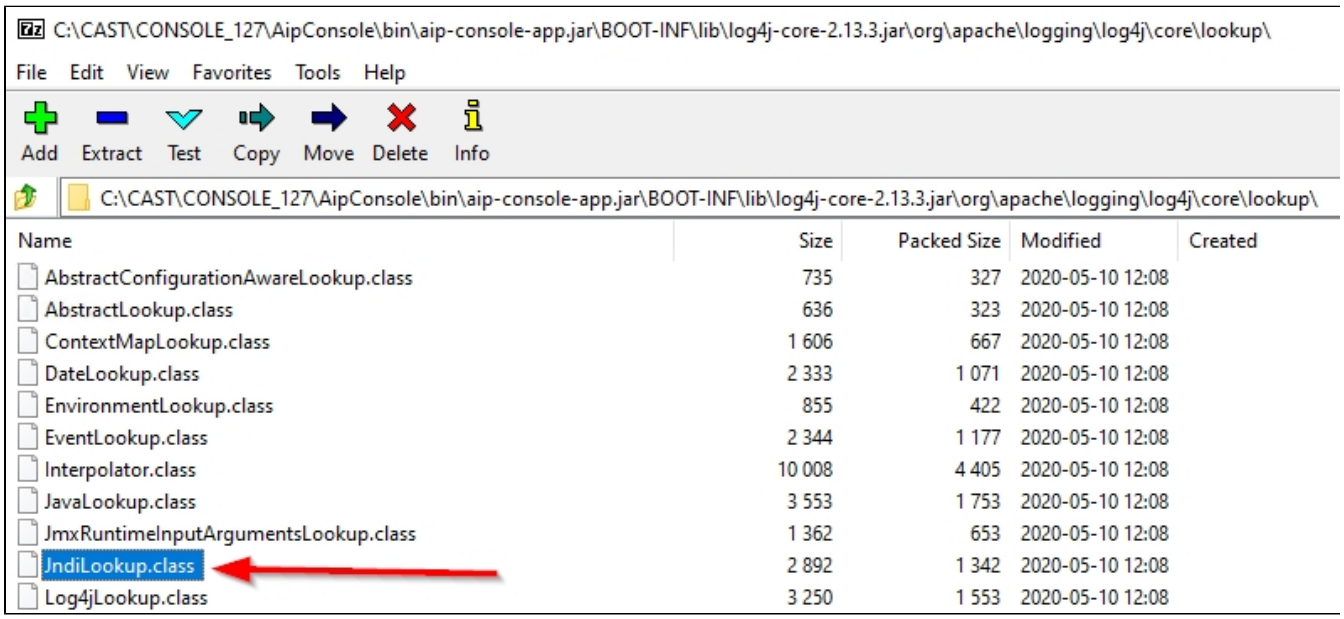
Open the .JAR files with **7Zip** (use the right click **Open Archive** option):



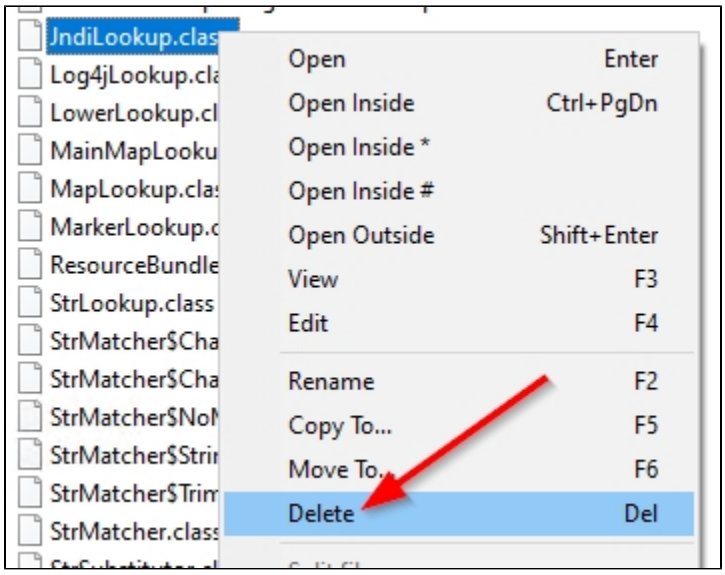
Drill down to the following location: **\BOOT-INF\lib** and locate the **log4j-core-*.jar** file:



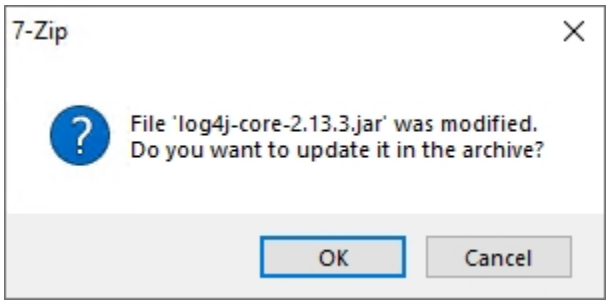
Click into this file and drill down to the following location: **org\apache\logging\log4j\core\lookup** and locate the **JndiLookup.class** file:



Delete this file using the right click menu option:



Now close the 7Zip window. You will be prompted with the following message:



Click **OK** and 7Zip will automatically recompile the **log4j-core-*.jar** and the parent **aip-console-app.jar / aip-node-app.jar** file. Now restart the AIP Console service and all AIP Node services to ensure the change is taken into account.

Linux (AIP Console service only)

Locate the following file:

```
$HOME/CAST/AIPConsole/AIPConsole/bin/aip-console-app.jar
```

Create a temporary folder and unzip this .JAR file into a new empty folder:

```
mkdir temp
unzip aip-console-app.jar -d $HOME/CAST/AIPConsole/AIPConsole/bin/temp
```

Now move into the temporary folder and sub folders of the unzipped parent .JAR and run the following command to remove a .class file from a the Log4j core JAR file located in the folder:

```
cd temp/BOOT-INF/lib
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Now navigate back to the parent temporary folder you created earlier and zip the contents of the folder into a new **aip-console-app.jar** file:

```
zip -r aip-console-app.jar *
```

Now copy the new **aip-console-app.jar** file into the original location of this file, replacing the original:

```
cp aip-console-app.jar $HOME/CAST/AIPConsole/AIPConsole/bin/
```

Now restart the AIP Console service and all AIP Node services to ensure the change is taken into account.

CAST Imaging

Edit the following file:

```
Microsoft Windows traditional installer:
%APPDATA%\CAST\ImagingSystem\neo4j\neo4j.conf

Docker Installer extension (located in the folder created when unzipping the extension):
neo4j\configuration\neo4j.conf
```

Add the following lines to the end of the file and then save the file:

```
dbms.jvm.additional=-Dlog4j2.formatMsgNoLookups=true
dbms.jvm.additional=-Dlog4j2.disable.jmx=true
```

Restart the **Neo4j Windows service** / **Docker container** to ensure the changes are taken into account.