Apache Log4j - CVE vulnerabilities

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

Introduction

Several serious vulnerabilities have been found recently in **Apache Log4j** (the java based logging utility):

- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228** - present in **Apache Log4j 2.0 - 2.14.1**
- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046** - present in **Apache Log4j 2.0 - 2.15.0**
- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105** - present in **Apache Log4j 2.0 - 2.16.0**
- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832** - present in **Apache Log4j 2.0 - 2.17.0**

See also **https://logging.apache.org/log4j/2.x/security.html**.

Any Java application that makes use of Apache Log4j version **2.0 - 2.17** is impacted by these vulnerabilities. Apache has fixed all currently known vulnerabilities in **Apache Log4j 2.17.1**. CAST makes use of **Apache Log4j 2.0 - 2.16** in various products, therefore this page explains:

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

Which CAST products are affected?

Affected product	Affected by CVE-2021-44228	Affected by CVE-2021-45046	Affected by CVE-2021-45105 and CVE-2021-44832
CAST Dashboards /RestAPI	All releases (up to **2.4.0-funcrel**) 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 any release of AIP Console - CAST Security Dashboard standalone	All releases (up to **2.4.1-funcrel**) 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 any release of AIP Console - CAST Security Dashboard standalone	All releases (up to **2.4.3-funcrel**) 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 any release of AIP Console - CAST Security Dashboard standalone

CAST AIP Console	All releases (up to **1.26.0-funcrel** and **2.0.0 -beta 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	All releases (up to **1.26.1-funcrel** and **2.0.0 -beta 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	All releases (up to **1.27.0-funcrel** and **2.0.0-beta 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
CAST Imaging	All releases from **2.2.0-beta1** up to **2.7.0-funcrel**. The vulnerability is found in the third-party software **Neo4j 4.2.**		All releases from **2.2.0-beta1** up to **2.7.1-funcrel**. The vulnerability is found in the third-party software **Neo4j 4 .2.**
AIP Core: CAST Management Studio	All releases up to **8.3.41**. The vulnerability is found in an embedded WAR file used in CAST Management Studio.		
JEE Analyzer extension	All releases up to **1.3.5-funcrel**. The analyzer provides Environment Profiles to handle specific frameworks and a legacy Log4j JAR (**1.12.4**) is provided in **%PROGRAMDATA%\CAST\CAST\Extensions\com.castsoftware.jee.1.3.5-funcrel\EnvProf\J2EE\Log4j**.		
Delivery Folder Migration Tool	All releases up to **1.0.3-funcrel**.		All releases up to **1.0.4-funcrel**.
Security for Java extension	All releases up to **1.6.5-funcrel**.		All releases up to **1.6.6-funcrel**.
PHP extension	All releases up to **3.1.0-beta**. The vulnerability is located in the **pre-processor** (Configuration\Languages\PHP\prepro folder).		
Message Queues extension	All releases up to **1.2.2-funcrel**. The vulnerability is located in the shipped **RabbitMQ** jars (jars\RabbitMQ_jars folder).		

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 2.16.0** / **2.17.0** / **2.17.1** which include the fixes for these vulnerabilities. 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 2.16.0**	**Release containing Apache Log4j 2.17.0 / 2.17.1**

CAST Dashboards /RestAPI	**2.4.3-funcrel** Released **16 Dec 2021.** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard&version=2.4.3-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.health&version=2.4.3-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.engineering&version=2.4.3-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.security&version=2.4.3-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.restapi&version=2.4.3-funcrel** **1.28.4-funcrel** Released **15 Dec 2021**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard&version=1.28.4-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.health&version=1.28.4-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.engineering&version=1. 28.4-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.security&version=1.28.4-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.restapi&version=1.28.4-funcrel**	**2.5.0-funcrel** Released **11 Jan 2022**. Contains **Log4j 2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard&version=2.5.0-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.health&version=2.5.0-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.engineering&version=2.5.0-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.security&version=2.5.0-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.restapi&version=2.5.0-funcrel** **1.28.5-funcrel** Released **11 Jan 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard&version=1.28.5-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.health&version=1.28.5-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.engineering&version=1. 28.5-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.security&version=1.28.5-funcrel** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.dashboard.restapi&version=1.28.5-funcrel**
CAST AIP Console	**1.27.0-funcrel** Released **17 Dec 2021**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.console&version=1.27.0-funcrel**	**2.0.0-funcrel** Released **12 Jan 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.console&version=2.0.0-funcrel** **1.27.1** Released **18 Feb 2022**. Contains Log4j **2.17.1.** • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip.console&version=1.27.1-funcrel**
CAST Imaging	**2.7.1-funcrel** Released **20 Dec 2021**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.imaging&version=2.7.1-funcrel** ⓘ If this release is installed as Linux Docker containers, release **1.2.4-funcrel** of the **Docker Installer** extension is also required.	**2.8.1-funcrel** Released **28 Jan 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.imaging&version=2.8.1-funcrel**
AIP Core: CAST Management Studio	N/A	**8.3.42** Released **28 Jan 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com. castsoftware.aip&version=8.3.42**

ⓘ

JEE Analyzer extension	N/A	ⓘ No fix will be applied to the 1.0 or 1.1 branches. **1.3.6-funcrel** Released **25 Feb 2022**. Contains Log4j **2.17.1**. **https://extend.castsoftware.com/#/extension?id=com.castsoftware.jee&version=1.3.6-funcrel** **1.2.23 (LTS)** Released **18 Mar 2022**. Contains Log4j **2.17.1**. **https://extend.castsoftware.com/#/extension?id=com.castsoftware.jee&version=1.2.23**
Delivery Folder Migration Tool	**1.0.4-funcrel** Released **15 Dec 2021**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.console.delivery.folder.migration.tool&version=1.0.4-funcrel**	**1.0.5-funcrel** Released **15 Apr 2022**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.console.delivery.folder.migration.tool&version=1.0.5-funcrel**
Security for Java extension	**1.6.6-funcrel** Released **20 Dec 2021**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.securityforjava&version=1.6.6-funcrel**	**1.6.7-funcrel** Released **24 Jan 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.securityforjava&version=1.6.7-funcrel**
PHP extension	N/A	**3.1.2-funcrel** Released **08 April 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.php&version=3.1.2-funcrel** **3.1.0-funcrel** Released **22 Dec 2021**. Contains Log4j **2.17.0**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.php&version=3.1.0-funcrel**
Message Queues extension	N/A	**1.2.3-funcrel** Released **31 Jan 2022**. Contains Log4j **2.17.1**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.mqe&version=1.2.3-funcrel**

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 2.16.0** or **2.17.0/2.17.1**, you can perform the actions listed below to mitigate the vulnerability.

⚠ Previous advice given in this page about using a Microsoft Windows environment variable to set **LOG4J_FORMAT_MSG_NO_LOOKUPS = true** or to pass **-Dlog4j2.formatMsgNoLookups=true** as a Java parameter when launching CAST products have been found to be ineffective at stopping RCE in some situations, explained here **by Apache** and in **CVE-2021-45046**.

In addition, other advice previously given to manually remove the **JndiLookup.class** file has been found to cause errors when restarting some CAST products.

As such this documentation has been removed. The only known reliable methods of mitigating the threat at this time (where upgrading to a new release of CAST products containing Apache Log4j 2.16.0 / 2.17.0 / 2.17.1 is not possible or not available) is to **manually patch your installation with Apache Log4 2.17.0 / 2.17.1** (as explained below).

CAST Dashboards/RestAPI

Before starting:

- ensure that you **stop** any running services.
- download and extract either:
  - the **Apache Log4j 2.17.0** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.0/apache-log4j-2.17.0-bin.zip** (approx 15MB).
  - the **Apache Log4j 2.17.1** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.1/apache-log4j-2.17.1-bin.zip** (approx 14MB).
- the instructions include a step which requires the use of the Java "jar" command. This command is only recognised when you have installed a Java JDK. If you only have the JRE, then the command will fail.
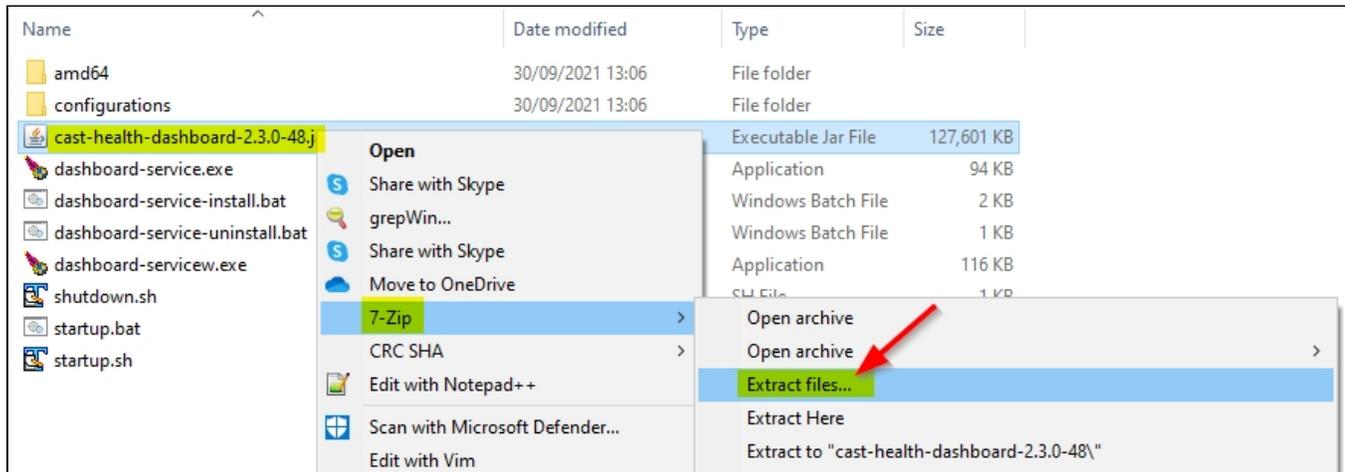
ZIP file deployment (2.0.0-funcrel)

Find the following file:

```
<unpacked_zip>\<dashboard>-<version>.jar
```

Microsoft Windows action

Extract the .JAR file with **7Zip (use the right click Extract files... option)** to a temporary folder for example **C:\CAST\temp**

When extracted, drill down to the following location: **C:\CAST\temp\<folder>\BOOT-INF\lib** and locate the four files listed below. **Delete these four files** and then **replace** them with the **equivalent 2.17.0/2.17.1 files located in the ZIP you downloaded from Apache**:

- **log4j-api-*.jar**
- **log4j-core-*.jar**
- **log4j-jul-*.jar**
- **log4j-slf4j-impl-*.jar**
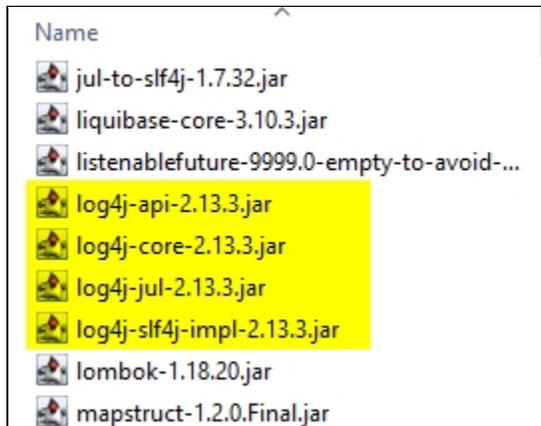
Open a command prompt using **CMD** and navigate to **C:\CAST\temp\<folder>**. Run the command listed below in the CMD window. This action will generate **a new .JAR file containing the updated Apache Log4j 2.17.0/2.17.1 files**. Ensure you define the **correct name** for the .jar file - it must match the name used in the default installation:

```
jar cMvf0 <dashboard>-<version>.jar *
```

ⓘ Note that the "jar" command is only recognised when you have installed a Java JDK. If you only have the JRE, then the command will fail.

You now need to copy this new .JAR file into the original **unpacked Dashboard ZIP installation folder** and overwrite the original file. **Restart** the CAST Dashboard to ensure the change is taken into account.

Linux action

Create a temporary folder and unzip the **<unpacked_zip>/<dashboard>-<version>.jar** file into this new empty folder:

```
mkdir $HOME/CAST/temp
unzip path/to/<unpacked_zip>/<dashboard>-<version>.jar -d $HOME/CAST/temp
```

Delete the following four files located in the **BOOT-INF/lib/** folder in the folder containing the extracted CAST Dashboard .JAR:

- **log4j-api-*.jar**
- **log4j-core-*.jar**
- **log4j-jul-*.jar**
- **log4j-slf4j-impl-*.jar**

```
cd $HOME/CAST/temp/BOOT-INF/lib/
rm -rf log4j-api-*.jar log4j-core-*.jar log4j-jul-*.jar log4j-slf4j-impl-*.jar
```

Copy the equivalent four **2.17.0 files** located in the ZIP you downloaded from Apache into the extracted **BOOT-INF/lib/** folder:

```
cp $HOME/CAST/<unpacked_Apache_ZIP>/{log4j-api-2.17.0.jar,log4j-core-2.17.0.jar,log4j-jul-2.17.0.jar,log4j-slf4j-impl-2.17.0.jar} $HOME/CAST/temp/BOOT-INF/lib/
```

Navigate into the folder containing the extracted CAST Dashboard .JAR and run the command listed below. This action will generate **a new .JAR file containing the updated Apache Log4j 2.17.0/2.17.1 files**. Ensure you define the correct name for the .jar file - it must match the name used in the default installation:

```
cd $HOME/CAST/temp
jar cMvf0 <dashboard>-<version>.jar *
```

ⓘ Note that the "jar" command is only recognised when you have installed a Java JDK. If you only have the JRE, then the command will fail.

Copy the new **<dashboard>-<version>.jar** file into the original location of this file, replacing the original:

```
cp <dashboard>-<version>.jar path/to/<unpacked_zip>
```

Restart the CAST Dashboard to ensure the change is taken into account.

Apache Tomcat deployment (any release)

Browse to the following location:

```
CATALINA_HOME\webapps\<dashboard>\WEB-INF\lib\
```

Delete these four files and then **replace** them with the **equivalent 2.17.0/2.17.1 files located in the ZIP you downloaded from Apache**:

| CAST Dashboards 1.x | CAST Dashboards 2.x |

• **log4j-api-*.jar** • **log4j-core-*.jar** • **log4j-jcl-*.jar** • **log4j-web-*.jar**	• **log4j-api-*.jar** • **log4j-core-*.jar** • **log4j-jul-*.jar** • **log4j-slf4j-impl-*.jar**

Restart the CAST Dashboard to ensure the change is taken into account.

CAST AIP Console

Before starting note the following:

- ensure that you **stop** any running services.
- download and extract either:
    - the **Apache Log4j 2.17.0** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.0/apache-log4j-2.17.0-bin.zip** (appro x 15MB).
    - the **Apache Log4j 2.17.1** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.1/apache-log4j-2.17.1-bin.zip** (appr ox 14MB).
- the instructions include a step which requires the use of the Java "jar" command. This command is only recognised when you have installed a Java JDK. If you only have the JRE, then the command will fail.
- restart the relevant services to ensure that the changes are taken into account.

Microsoft Windows (AIP Console front-end and AIP Node back-end)

Log4j files are found in two locations:

Location 1

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

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

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

Extract each .JAR file with **7Zip** (use the right click **Extract files...** option) to a temporary folder (use **one folder for each JAR**), for example **C: \CAST\temp\<folder>**:
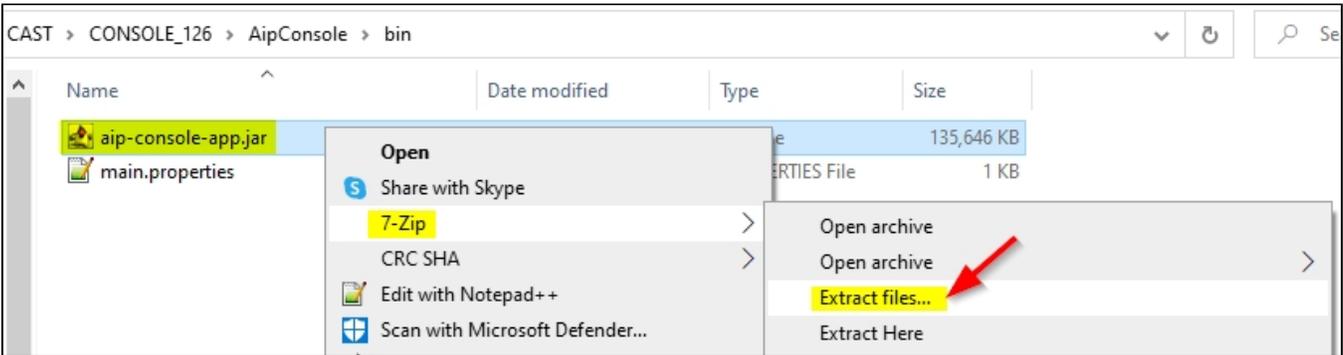
When extracted, drill down to the following location: **C:\CAST\temp\<folder>\BOOT-INF\lib** in each extracted folder and locate the four files listed below. **Delete these four files** and then **replace** them with the **equivalent 2.17.0/2.17.1 files located in the ZIP you downloaded from Apache**. Repeat for each AIP Console .JAR file you have extracted.

- **log4j-api-*.jar**
- **log4j-core-*.jar**
- **log4j-jul-*.jar**
- **log4j-slf4j-impl-*.jar**
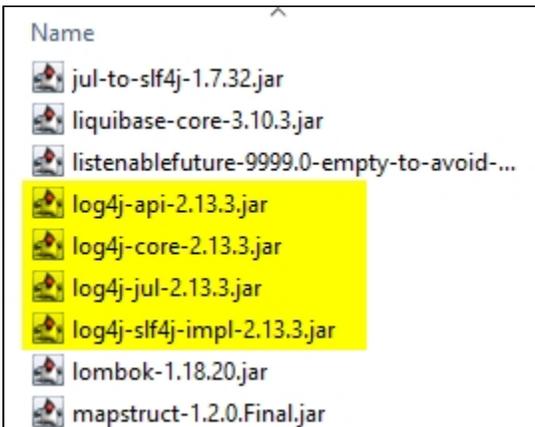
Open a command prompt using **CMD** and navigate to **C:\CAST\temp\<folder>**. Run the command listed below in the CMD window. Repeat for each AIP Console/Node .JAR file you have extracted. This action will generate **a new .JAR file containing the updated Apache Log4j 2.17.0/2.17.1 files**:

```
jar cMvf0 aip-console-app.jar *
```

> ⓘ Note that the "jar" command is only recognised when you have installed a Java JDK. If you only have the JRE, then the command will fail.

You now need to copy this new .JAR file to the relevant CAST AIP Console/Node installation folder under **/bin** and overwrite the original.
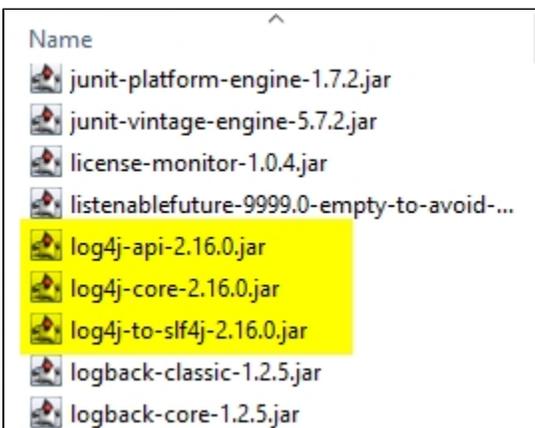
Location 2

Browse to the following location on all AIP Node services:

```
%PROGRAMFILES%\CAST\AipConsole\AipNode\admin\bin\lib
```

Locate the three files listed below. **Delete these files** and then **replace** them with the **equivalent 2.17.0/2.17.1 files located in the ZIP you downloaded from Apache**. Repeat for each AIP Node service:

- **log4j-api-*.jar**
- **log4j-core-*.jar**
- **log4j-to-slf4j-*.jar**

Linux (AIP Console service only)

Locate the following file:

```
<AIPConsole_install>/bin/aip-console-app.jar
```

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

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

Delete the following four files located in the **BOOT-INF/lib/** folder in the folder containing the extracted AIP Console .JAR:

- **log4j-api-*.jar**
- **log4j-core-*.jar**
- **log4j-jul-*.jar**
- **log4j-slf4j-impl-*.jar**

```
cd $HOME/CAST/temp/BOOT-INF/lib/
rm -rf log4j-api-*.jar log4j-core-*.jar log4j-jul-*.jar log4j-slf4j-impl-*.jar
```

Copy the equivalent four **2.17.0 files** located in the ZIP you downloaded from Apache into the extracted **BOOT-INF/lib/** folder:

```
cp $HOME/CAST/<unpacked_Apache_ZIP>/{log4j-api-2.17.0.jar,log4j-core-2.17.0.jar,log4j-jul-2.17.0.jar,log4j-
slf4j-impl-2.17.0.jar} $HOME/CAST/temp/BOOT-INF/lib/
```

Navigate into the folder containing the extracted AIP Console .JAR and run the command listed below. This action will generate **a new .JAR file containing the updated Apache Log4j 2.17.0/2.17.1 files**:

```
cd $HOME/CAST/temp
jar cMvf0 aip-console-app.jar *
```

ⓘ   Note that the "jar" command is only recognised when you have installed a Java JDK. If you only have the JRE, then the command will fail.

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

```
cp aip-console-app.jar <AIPConsole_install>/bin
```
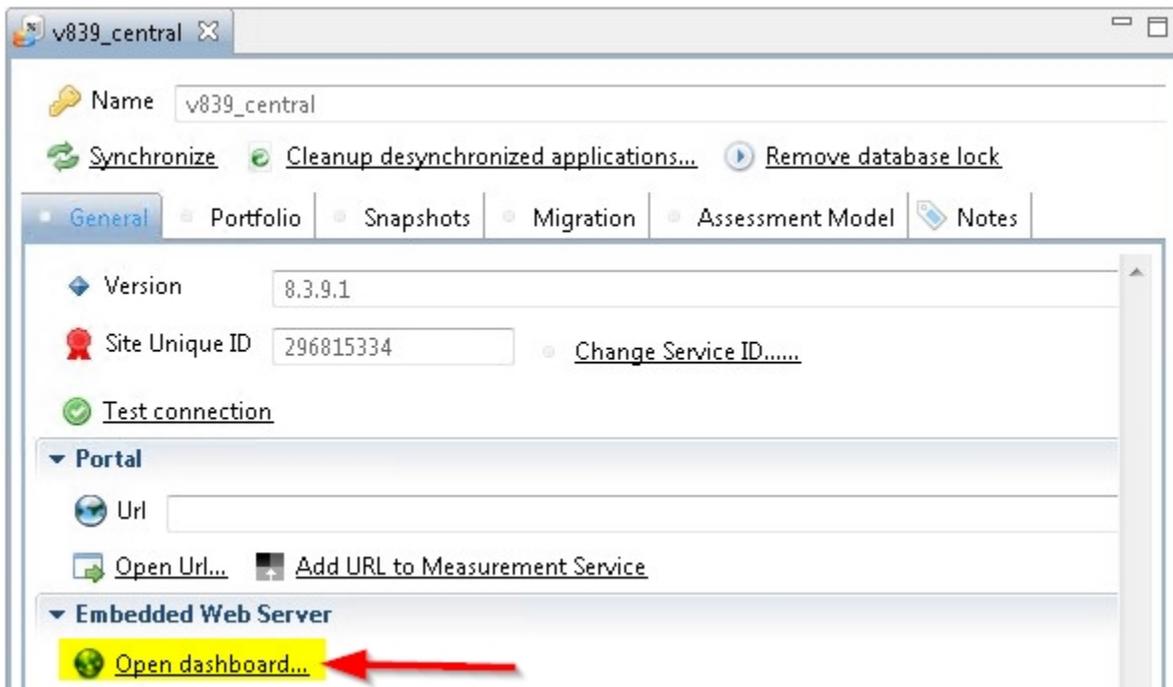
AIP Core: CAST Management Studio

Before starting note the following:

- close CAST Management Studio if is already open.
- download and extract either:
    - the **Apache Log4j 2.17.0** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.0/apache-log4j-2.17.0-bin.zip** (approx 15MB).
    - the **Apache Log4j 2.17.1** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.1/apache-log4j-2.17.1-bin.zip** (approx 14MB).

Introduction

CAST Management Studio includes an **embedded WAR** file that is used by this option:

When the option is clicked, the embedded WAR file is launched on the fly and it is this WAR file that contains Log4j files. To mitigate this, there are two steps listed below:

Clean up temporary files

When the option is clicked, CAST Management Studio deploys the embedded WAR file in the following location - the deployed location will contain the Log4j files (as well as being present in the WAR file):

```
%TEMP%\jetty-0_0_0_0-0-CAST-AED-CMS_war-_CAST-AED-CMS-any-<random_id>.dir
```

You should first delete this folder entirely.

Replace existing Log4j JAR files

Browse to the following location and locate the embedded WAR file:

```
%PROGRAMFILES%\CAST\8.3\WARS\internal\CAST-AED-CMS.war
```

Extract the WAR file using **7Zip** (use the right click **Extract files...** option) to a temporary folder, for example **C:\CAST\temp\<folder>**. When extracted, drill down to the following location: **C:\CAST\temp\<folder>\WEB-INF\lib** and locate the four files listed below. **Delete these four files** and then **replace** them with the **equivalent 2.17.0/2.17.1 files located in the ZIP you downloaded from Apache**:

- **log4j-api-*.jar**
- **log4j-core-*.jar**
- **log4j-jcl-*.jar**
- **log4j-web-*.jar**
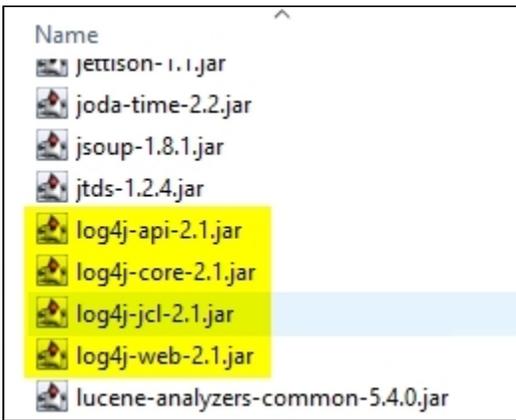
Now archive the extracted files and create a new WAR file called **CAST-AED-CMS.war** using **7Zip**:
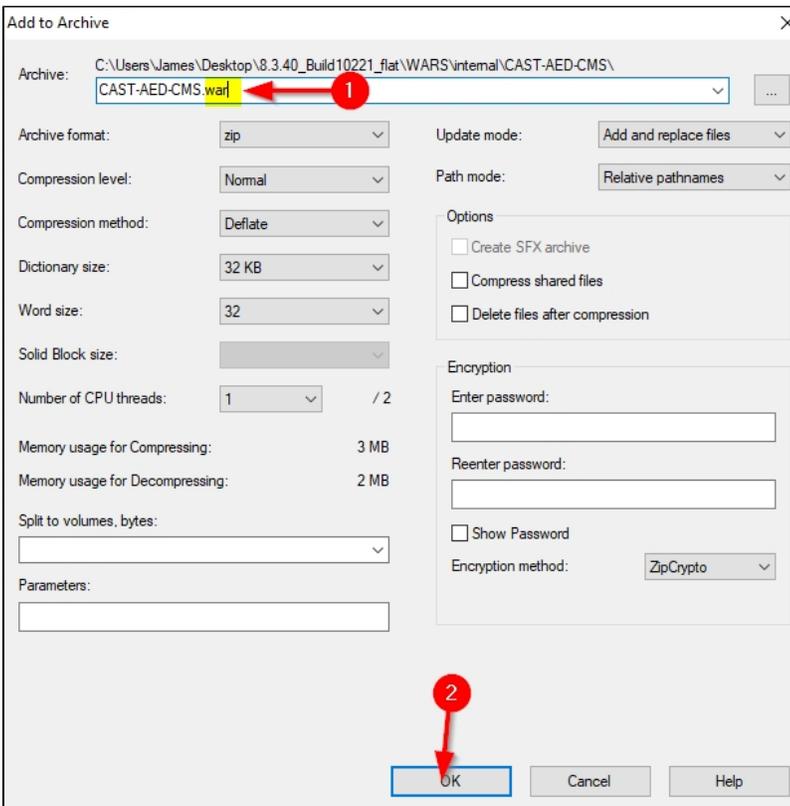
Copy the resulting .WAR file and paste it into the following location, overwriting the existing WAR file:

```
%PROGRAMFILES%\CAST\8.3\WARS\internal\CAST-AED-CMS.war
```

The next time you use the **Open dashboard** option in CAST Management Studio, the newly created WAR file will be deployed to %TEMP% and then used.

Message Queues extension

Before starting note the following:

- ensure that you are not currently running an analysis that uses this extension.
- download and extract either:
    - the **Apache Log4j 2.17.0** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.0/apache-log4j-2.17.0-bin.zip** (appro x 15MB).
    - the **Apache Log4j 2.17.1** patch from **https://www.apache.org/dyn/closer.lua/logging/log4j/2.17.1/apache-log4j-2.17.1-bin.zip** (appr ox 14MB).

Browse to the following location in the installed extension on all AIP Nodes:

```
%PROGRAMDATA%\CAST\CAST\Extensions\com.castsoftware.mqe.<version>\jars\RabbitMQ_jars
```

Locate the two files listed below. **Delete these files** and then **replace** them with the **equivalent 2.17.0/2.17.1 files located in the ZIP you downloaded from Apache**. Repeat for each AIP Node service where this extension is installed:

- **log4j-api-*.jar**
- **log4j-to-slf4j-*.jar**