Procedure to mitigate the risk concerning the CVE-2021-44228 vulnerability.

Please find below the tested and validated procedure to mitigate the risk concerning the CVE-2021-44228 vulnerability.

In your installation base, please search for the following file: *log4j-core*.jar

- If you do not find any result, you can stop the procedure here. Your installation is not vulnerable
- If you find a match, the log4j2 library is installed and could be exploited. Please execute these steps:
    - Download log4j v2.15.0 from apache website (link)
    - Search now for all the additional jar files (see complete list at the bottom) and replace any match by the 2.15.0 version. **Make sure the original filename is unchanged.**
    - The replacing and renaming operations must be performed for all jar files found from the list

Example#1 (with version number in the name):

If you find log4j-core-2.11.2.jar:

1. Remove log4j-core-2.11.2.jar
2. Copy log4j-core-2.15.0.jar to the same location
3. Rename log4j-core-2.15.0.jar to log4j-core-2.11.2.jar

Example#2 (without any version number in the name):

If you find log4j-docker.jar:

1. Remove log4j-docker.jar
2. Copy log4j-docker.jar to the same location
3. Rename log4j-docker.jar to log4j-docker.jar

Complete list of jar files to look for if *log4j-core*.jar is found:

- *log4j-1.2-api*.jar
- *log4j-api*.jar
- *log4j-appserver*.jar
- *log4j-cassandra*.jar
- *log4j-core*-tests.jar
- *log4j-core*.jar
- *log4j-couchdb*.jar
- *log4j-docker*.jar
- *log4j-flume-ng*.jar
- *log4j-iostreams*.jar
- *log4j-jcl*.jar
- *log4j-jdbc-dbcp2*.jar
- *log4j-jmx-gui*.jar
- *log4j-jpa*.jar
- *log4j-jul*.jar
- *log4j-liquibase*.jar
- *log4j-mongodb3*.jar
- *log4j-mongodb4*.jar
- *log4j-slf4j-impl*.jar
- *log4j-slf4j18-impl*.jar
- *log4j-spring-boot*.jar
- *log4j-spring-cloud-config-client*.jar
- *log4j-taglib*.jar
- *log4j-to-slf4j*.jar
- *log4j-web*.jar

Please restart the system