Releases - DissFTP package

Lately, the critical Apache Log4j vulnerability CVE-2021-44228 in the Apache Log4j library has been announced.

The DissFTP Server is using Apache Log4j v1.x which is not directly affected by the Log4shell vulnerability. There is still a possibility of being hit by the JNDI issue but only if the JMS appender was configured in the "log4j.properties" files, which is definitely not the case. However, if you are really concerned, you can always add the following lines in the "dissftpd" startup script (along with the other java options):

```
JAVA_OPTS=$JAVA_OPTS" -Dcom.sun.jndi.rmi.object.trustURLCodebase=false"
JAVA_OPTS=$JAVA_OPTS" -Dcom.sun.jndi.cosnaming.object.trustURLCodebase=false”
```

And restart the daemon to apply the change.

The minimum requirement for the DissFTP package is Java1.6.x, however we recommend installing the latest JDK from Oracle available at the following URL:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

The DissFTP software is currently running at ECMWF using the Oracle Java version "1.8.0_60" - Java HotSpot(TM) 64-Bit Server VM (build 25.60-b23, mixed mode).

Ecaccess DissFTP package v1.1.0 (Java 1.6+)