Log4J Remote Code Execution Vulnerability

2021-12-14 - Jason Gillan - Comments (0) - General

No Formpipe Products are vulnerable to the Log4J exploit. Further details are below.

A remote code execution vulnerability (CVE-2021-44228) has recently been identified in Log4J, an open-source logging library for Java.

As soon as reports of this vulnerability started appearing online, Formpipe investigated all products to analyse the potential threat to anyone with a Formpipe product installed.

It was found the only direct usage of Log4J within Formpipe products is in the Temenos interfaces, however, these use Log4J 1.x which is not affected. The DM and BPM products use logging facades (Slf4J) which in turn use the logging subsystem within Wildfly (the application server Autoform DM and BPM run on), however, the JBoss logging implementation that is used under the covers has not been identified to contain the vulnerability.

The key takeaway is that all products (DM, BPM, Interfaces) are not affected and no other Formpipe products use Log4J.

If anyone has replaced the Log4J library that is installed with Autoform DM to one of the libraries with the vulnerability, it is advised to contact Formpipe Support immediately for our assistance in fixing this.

As well as that, Java versions greater than 6u211, 7u201, 8u191, and 11.0.1 aren't affected by this attack vector. This covers all versions of Autoform DM 9.0 and newer.

For clarity, these are the versions of Autoform DM and which JDK they ship with:

- DM 9.0+ - 11.0.4_11
- DM 8.3.0+ - 1.8.0_151 (RMI)
- DM 8.2.0+ - 1.8.0_144 (RMI)
- DM 8.0.0+ - 1.8.0_112 (JNDI/RMI)
- Temenos interfaces use the JDK of the Transact environment.
- BPM uses an older JDK 8 version: 1.8.0_45 and continues to do so.