Log4J 1.x JSM Appender and Log4Net Vulnerabilities

2022-01-13 - Alex Clemons - Comments (0) - Autoform DM News

Following on from the recent vulnerabilities reported last month with Log4J it has since been reported that there are additional vulnerabilities with different versions of Log4J. During this investigation, we have also identified a potential vulnerability with the Log4Net used for logging in some of the other products used in conjunction with Autoform DM.

After a thorough analysis, it has been found that the following products are affected by these new vulnerabilities. Any product not mentioned below is not affected by these vulnerabilities:

Log4J
The initial vulnerability found in Log4J only affected the 2. x versions. Since then a new one was discovered in the JMS Appender within Log4J 1. x (https://nvd.nist.gov/vuln/detail/CVE-2021-4104).

By default, the JMS Appender is not configured within Formpipe Products and we have never recommended that anyone should configure it. In order to exploit this vulnerability, an attacker would have to have access to the logging configuration file, reconfigure logging and then restart the service.

Although for the sake of complete openness and security, it is possible to remove the appender in question by removing the **Org/apache/log4j/net/JMSAppender.class** file from the **Log4J** file.

This includes the Log4J distribution supplied within Autoform DM's Wildfly implementation, the Temenos Interfaces and jFinder.

Log4Net

While reviewing Apache libraries, it has also been identified that some Formpipe Products are running older versions of Log4Net with a potential vulnerability (https://nvd.nist.gov/vuln/detail/CVE-2018-1285) which would allow an attacker to perform an XXE (XML External Entity Reference) attack if able to supply a configuration file to an application. This has no relation to the recently identified Log4Shell vulnerability which targets Log4J.

This affects Log4Net versions prior to 2.0.10 of which a number of the .Net based applications use. However, the vulnerability specifically requires the ability for the attacker to provide a configuration file at runtime. Having analysed the affected applications, we can confirm that none of them support this and thus do not provide a means by which to exploit the issue.

As such this is classified as *low risk*. For anyone concerned about the issue, we recommend that they review our standard security recommendations - namely to ensure application installations are protected with appropriate file permissions and access controls, and that user access follows the principal of *Least Privilege*.

Future releases will ensure that we no longer use the affected version.

Each product affected will be listed below:

- Autoform DM Client, Application Editor and .net Applications
- Temenos CBS
- Service Bus Loader
- Service Bus Processor
- DM Upload (more information below)

DM Upload in Lasernet

DM Upload is a module included in Lasernet 9 and 10, replacing the older DM Archive module:

This module uses Log4Net as a logging library and has a new version released with an updated library. While new releases of Lasernet will contain this fix, it can also be manually updated using the files available here:

https://formpipe.support/DM_Upload

The files can be extracted and copied in place of the current DM Upload module files either in:

C:\Program Files\Formpipe Software\Lasernet 9\Modules.NET\Lasernet DM Upload Module

Or:

C:\Program Files\Formpipe Software\Lasernet 10\Modules.NET\Lasernet DM Upload Module

- Depending on the version of Lasernet used.