Subject: Log4j
Posted by eh2021 on Fri, 30 Dec 2022 20:48:40 GMT
View Forum Message <> Reply to Message

Hello,

We are seeing the opsin.jar file used for DataWarrior being flagged as vulnerable to Log4j. Is this file actually vulnerable and is it needed for software functionality?

Subject: Re: Log4j
Posted by thomas on Sat, 31 Dec 2022 16:56:55 GMT
View Forum Message <> Reply to Message

I am not an expert, but according to my understanding, the log4j problem primarily hits servers, which use log4j to write log entries under certain circumstances. If a log message contained a certain type of URL, then a previous version of log4j used to download Java code from an external server and execute it. If an external user was able cause a server log entry to be written that would contain a hostile URL he had entered somewhere, he could run code on that machine and, thus, gain access.

The capka.jar does not expose functionality to people external of you desktop computer. Therefore, I don't see a risk that some external user communicate from outside to your computer's running DataWarrior instance, cause the generation of custom tailored log entries written by the capka.jar to gain access to the machine.

The capka.jar file does not belong to the standard DataWarrior installation, but if you download it from ChemAxon and add it to the DataWarrior lib folder, DataWarrior can use to calculate pKa values and other properties, which depend on the pKa value.

The critical file (within a jar file) causing the log4j problem is supposedly: org/apache/logging/log4j/core/lookup/JndiLookup.class. Therefore, a quick remedy is to remove that file from the log4j code. capka.jar (27 June 2022, 12’926’671 bytes) does not contain such a file, although some other log4j code is inside.

I personally wouldn't see any risk using that file.