inrule

December 16, 2021

Statement regarding Apache Log4J utility exploit

InRule Technology is committed to providing secure, scalable services to our customers. We have reviewed the report CVE-2021-44228, announced on December 9, 2021, regarding the Apache Log4J utility exploit, which results in remote code execution (RCE).

We have completed a process of examining our code bases to ensure our customers are not impacted by this exploit. The following is a report, by component, for each of InRule Technology's AI-enabled end-to-end automation products.

InRule Decision Platform

InRule for Java. The code base for both InRule for Java, and our Java Distribution Service are not affected.

Customer Instances. No production instances of the InRule Decision Platform use Log4j anywhere in its code base. The identified vulnerability is not a concern for decision platform customers.

Trial Instances. Trials initiated after mid-November 2021 have a decision lifecycle analytics feature. We have confirmed no attack vectors are open from outside the application. Our team is working with our partners to perform any necessary mitigation; however please be aware no customer data is stored as part of the lifecycle analytics feature in trials.

xAI Workbench

Customer Instances and Trials. We have evaluated all code in our explainable machine learning platform, xAI Workbench and have confirmed it is not affected by the zero-day exploit.

Barium Live

Production Environment. Our Digital Process Automation (DPA) team has completed a thorough scan, evaluated any effects and if appropriate, performed any necessary mitigation. There should be no cause for concern for our DPA customers.