December 15, 2021

Product Information Notice (PIN): Apache Log4j CVE-2021-44228 Risk Assessment

Dear Impinj Customer,

On December 13, 2021, Impinj became aware of a critical security vulnerability in the Apache Log4j logging framework, CVE-2021-44228 which impacts Java-based applications. Security is very important to Impinj and we conducted an audit to determine the impact of this vulnerability on our products. We determined that no Impinj products are susceptible to CVE-2021-44228 and no action is needed by customers at this time. Results of the audit are below:

The following products and associated firmware do not include Java or the Log4j API and are not susceptible to CVE-2021-44228:

- Impinj R700 readers
- Impinj Speedway series readers
- Impinj xArray gateways
- Impinj xSpan gateways
- Impinj Speedway Connect software
- Impinj Indy series reader chips
- Impinj E710, E510, E310 reader chips
- Impinj tag chips

The following products do not utilize the Log4j API and are not susceptible to CVE-2021-44228:

- Impinj ItemSense software
- Impinj ItemEncode software

Impinj Octane SDK and Impinj Octane LTK Java development libraries use Log4j API version 1.2.17 which is not currently known to be susceptible to CVE-2021-44228. We continue to monitor the CVE as additional information becomes available. A forthcoming update to the Impinj Octane SDK and LTK will use Log4j API version 2.16 which is not susceptible to CVE-2021-44228. Additional communications will be provided when this update is available.

Best regards,

Jonathan Newkirk
Senior Product Manager
jnewkirk@impinj.com