PRINTRONIX

Log4j: Statement of Assurance - Printronix's product are not vulnerable

To Our Valued Printronix Customers,

We here at Printronix are fully aware of the issue and the concern and want to address any impact the Log4j threat has on the products we offer.

We are pleased to announce that after performing an internal review of our printer solutions, our engineering team has determined that neither our Printronix P8000 and S809/S828 printer firmware nor our PrintNet Enterprise (PNE) software utilizes the Log4j object library.

BACKGROUND

On November 24, 2021, a security gap was identified in the open-source code by Apache Software Foundation. It was then made public on 9 December 2021. It is estimated that the exploit affects hundreds of millions of devices and is very simple to execute. This gap allows hackers to carry out destructive cyberattacks by taking control of targeted computers/servers with remote-code execution that can cause Denial of Service (DOS), in addition to other damages.

References

- https://www.fastcompany.com/90706497/what-is-log4j-log4shell-cybersecurity-risk
- https://www.f5.com/labs/articles/threat-intelligence/explaining-the-widespread-log4j-vulnerability
- https://www.upguard.com/blog/apache-log4j-vulnerability

PRINTRONIX RECOMMENDED ACTIONS

Printronix customers do not have to take any additional action to address Log4j threat. But we recommend our customer adopt the following best practices:

- Install and maintain Printronix products (Printer and software) behind your corporate firewalls on a trusted network
- Do not recommend allowing access to any ports on these devices from the public Internet or from any untrusted network
- Allow only approved personal to access the product