



LOG4J 2 VULNERABILITY

Contact MCCi Technical Support at support@mccinnovations.com or call (866) 942-0464.

MCCi Products	Impacted	Additional Information
Managed Cloud (Infrastructure)	Not impacted	Review Complete
CWSAPI	Not impacted	Review Complete: Vendor Security Advisory link
PowerPack	Not impacted	Review Complete
GoFiche	Not impacted	Review Complete
Training Center	Not impacted	Review Complete
Laserfiche		
Self-Hosted (includes Managed Cloud & on-prem)	Not impacted	Review Complete: Vendor Security Advisory link
Laserfiche Cloud	Limited impact	Review Complete: Vendor Security Advisory link
Other		
Blue Prism	Not impacted*	<p>Review Complete: Vendor Security Advisory link</p> <p>Only clients who install and use the optional Blue Prism feature named "Data Gateways" and have updated Logstash or the Java Development Kit (JDK) to an affected version may be impacted.</p> <p>*MCCi does not enable this feature by default; however, clients can verify if the status of this feature by running bpserver.exe (Server Configuration application) and examining "enable Data Gateways process," which is found on either the Details tab (v6.x) or the Data Gateways Settings tab (v7.x)</p>
OneSpan	Impacted	<p>Under Review: being addressed two-fold.</p> <p>Vendor Security Advisory link</p> <p>They have configured their WAF to detect and block attempts to exploit the vulnerability. They also are working on updating their code to mitigate the vulnerability completely.</p>
Abbyy	Not impacted**	<p>Review Complete: Vendor Security Advisory link</p> <p>ABBYY has determined that this vulnerability does NOT impact its Cloud and on-premises products except for two database connectors: DBMS Connector for ABBYY Timeline and ABBYY FlexiCapture connector Pega.</p> <p>*MCCi does not deploy either of these connectors in our ABBYY-based solutions.</p>