NEWS RELEASE

Apache Log4j Cybersecurity Information

12/23/2021

Update: Notice on potential impact of Apache Log4j vulnerability towards Bio-Rad products and services
First published: December 23, 2021

Dear Bio-Rad Customer,

Bio-Rad understands the importance of security and is committed to managing its products and services with appropriate advanced security technologies for its customers worldwide.

Bio-Rad is aware of the reported Apache Log4j remote code execution vulnerability (CVE-2021-44228). Apache Log4j is an open-source logging JAVA-based library offered by Apache Software Foundation. Bio-Rad has investigated if any of our products and services may be potentially impacted by this vulnerability. More information about the vulnerability can be found here: **https://logging.apache.org/log4j/2.x/security.html**

Bio-Rad has surveyed and patched enterprise systems such as Bio-Rad.com to ensure protection against this vulnerability. In addition, we have found no evidence that any products are impacted by this vulnerability other than the one listed below.

Unity Connect 2:
Catalog Numbers 11000009, 11000010, 11000011, 11000012, 11000013

This product does not communicate directly with the internet, therefore we believe the risk to be low if the software is installed in a secure/protected environment. However, we do recommend that you upgrade to the newest version through Bio-Rad's QCNet website: **https://www.qcnet.com** to fully mitigate this vulnerability. Please contact your local IT team for assistance with the upgrade.

Bio-Rad is committed to supporting customers across the globe, enabling them to operate Bio-Rad products equipped with the latest security settings. In the event additional information becomes available regarding impacted Bio-Rad products, services and related countermeasures, we will provide them promptly on this page.

Erik Molitor
Chief Information Officer, Chief Information Security Officer
Bio-Rad Laboratories