Niagara Framework and the Apache log4j2 Vulnerability

ATTENTION ALL Lynxspring Business and Technical Partners

Last week, there was a CISA cybersecurity alert issued for a vulnerability discovered with Apache log4j2, a JAVA-based utility widely used by enterprise applications and cloud services offerings. See **CISA Cybersecurity Alert**.

Please be advised the Niagara Framework has been examined and evaluated to this vulnerability and all supported versions of the platform are unaffected. Furthermore, Lynxspring's JENEsys, JENEsys Edge, Onyxx and Onyxx LX products have displayed no dependencies and are not affected by this reported vulnerability.

As with all cybersecurity, please ensure the security robustness of your assets and your customers' assets. You should immediately investigate whether any modules developed by external or third-party vendors are installed in any station. If so, please contact those organizations to see if those modules are affected and develop a remediation plan if necessary.

Lynxspring is committed to taking a strong leadership role in helping our customers maintain a strong security posture by arming them with industry security information needed to be better prepared for possible cyber intrusions and providing the procedures, best practices, services, and higher level of security tools that help ensure the cyber protection of their systems, devices, applications, and data.

Thank you for your continued business and support.

Sincerely,

Marc Petock
Chief Marketing & Communications Officer
Lynxspring, Inc.
Phone: 877-649-5969
marc.petock@lynxspring.com
www.lynxspring.com
