TS PARTNERS

|630 Freedom Business Center Dr., Suite 212|
|King of Prussia, PA 19406|
|610.768.1100|

December 22, 2021

Apache Log4j Vulnerability - CVE-2021-44228 / CVE-2021-45046 / CVE-2021-45105

The Apache Software Foundation has released a security advisory to address a remote code execution vulnerability affecting Log4j versions. A remote attacker could exploit this vulnerability to take control of an affected system. Log4j is an open-source, Java-based logging utility widely used by enterprise applications and cloud services.

BACKGROUND

- TranStar application software (the system) is licensed to, and hosted locally by Clients
- TranStar is operated and controlled at/by Clients in their internal environment – Application and Database Server(s), Workstations, Network.
- LinkStar is the public-facing, web application Portal hosted by our Stock Transfer Clients for their Issuers to provide Shareholder Information Reporting and Proxy Processing.
- LinkStar is operated and controlled at/by Clients in their DMZ/web environment.

RESPONSE

TranStar: TS Partners evaluated the Log4j exploit threat. **TranStar is unaffected**:

- TranStar utilizes SLF4J (not Log4j) for logging purposes.
- TranStar does not utilize “log4j-core” and the Jar is not included in the build.

LinkStar: Web application is used by our Stock Transfer Clients in their Shareholder information reporting and Proxy processing. LinkStar uses SpringBoot framework that indirectly references Log4j.

- **LinkStar is unaffected.** It does not utilize “log4j-core” and the Jar is not included in builds.
- Vulnerability in “log4j-core” as “org/apache/logging/log4j/core/lookup/JndiLookup.class.”

While LinkStar does not include “log4j-core”, we have upgraded the bundled, companion “log4j-api” component to Apache 2.17.0 for all new LinkStar builds as a precaution.

SUMMARY

- This vulnerability does not affect Clients using Microsoft SQL Server as database engine.
- Log4j-core has been detected in Server installations at Clients that use Oracle 12, 18, 19 as database. Client IT should check for instances of “log4j-core” and patch as necessary.

For questions, please contact CEO or COO

Prior Review: December 15, 2021   Last Revision: December 22, 2021