TS PARTNERS

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

April 11, 2022

CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+

Background

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Apache Tomcat as a WAR servlet deployment. If the application is deployed as a Spring Boot executable jar, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

TS Partners and LinkStar Unaffected

This exploit requires that the target application be running via Tomcat as a Java web archive (WAR file). While LinkStar currently utilizes an affected version of the Spring Framework, LinkStar deployments only exist as executable jars. TS Partners does not distribute WAR deployments of LinkStar.

Out of an abundance of caution, the Spring Framework version used by LinkStar has been upgraded in our development branch. These changes will undergo testing and quality assurance consistent to TS Partners' standards.

Additional Information

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
Spring Framework RCE, Early Announcement

For questions regarding Policy, contact CEO or COO

Last Review: April 11, 2022
Last Revision: April 11, 2022