Non-impact of “Spring” Vulnerabilities:
Spring Cloud, Spring Expression, Spring Framework
CVE-2022-22950
CVE-2022-22963
CVE-2022-22965

Dimensional Insight Security Office &
Dimensional Insight Research and Development Laboratory

Overview

This week a vulnerability nick-named "Spring4Shell" or "SpringShell" was announced. The products under the "Spring" moniker are a popular web application framework implemented in Java. This vulnerability was assigned CVE identifier CVE-2022-22965. There were two other CVEs announced recently in these tools as well: CVE-2022-22950 and CVE-2022-22963.

Dimensional Insight software and cloud environment are **not vulnerable.** We do not make use of any Spring products.

Software and Platform Reviews

The DI Security and Development Teams immediately reviewed our software and our servers, and concluded that DI software is not vulnerable to this issue. Although our web applications, such as DivePort, are written partially in Java and run atop the Tomcat Java Web Application Server, we have never integrated Spring products into our software.

We also reviewed our cloud infrastructure, and found that Spring is not part of any other software installed on the DI Cloud and InteReport servers we host for our customers.

We found one internal IT system incorporating Spring, and have disabled it while we await specific information or software updates from its vendor. We determined it was not vulnerable to the worst of the issues, Spring4Shell, due to its runtime environment (JVM version). The other vulnerabilities may or may not be relevant. This system is not accessible from the Internet and access is heavily restricted internally. While the risk may be low or non-existent, we believe in exercising the utmost caution with Information Security.

DI continually reviews security announcements to see if any issues affect our products or cloud environment. We recommend that our self-hosted customers run Apache Tomcat version 9 or later, and monitor security announcements related to Tomcat and Java to protect their infrastructure.