Spring4Shell – Offizielle Stellungnahme von Collenda

Momentan existieren mehrere Hinweise zu Sicherheitslücken zum Java Spring Framework.

Konkret handelt es sich hierbei um die nachfolgenden Meldungen:

CVE-2022-22965, Spring4Shell, ermöglicht ggf. Remote Code Execution

CVE-2022-22950, ermöglicht ggf. DDoS Angriffe

CVE-2022-22963, Spring Cloud Function, ermöglicht ggf. Zugriff auf lokale Ressourcen

Wir haben seitens Collenda diese Meldungen bezogen auf unsere Anwendungsplattform OC4[1] analysiert. Das Spring Framework kommt in den nachfolgenden Modulen dort zum Einsatz:

Open Credit Loan Portal
Open Credit API Gateway
Open Credit Business Reporting

Ein besonderes Augenmerk hat in unseren Analysen die Meldung CVE-2022-22965 bekommen, da dort Möglichkeiten aufgezeigt werden, eine Remote Code Execution zu erreichen. Die in der Meldung skizzierten Angriffsvektoren können nicht gegen die im Einsatz befindliche Implementierung in den Collenda Modulen eingesetzt werden.

Die Meldung CVE-2022-22950 hat für Collenda Applikationen keine Relevanz, da der hier benötige Spring Expression Parser (SpEL) nicht zum Einsatz kommt.

Die Meldung CVE-2022-22963 hat für Collenda Applikationen keine Relevanz, da wir die Spring Cloud Funktionen nicht einsetzen.

Im Rahmen unserer Releasepflege der Collenda Applikationen werden wir als Vorsichtsmaßnahme Updates des Spring Frameworks vornehmen.

[1]Gilt auch für alle Versionen bekannt als Collenda Banknology, Collenda Banking, Financial Framework, die sich aktuell in Wartung befinden.