Service-Mitteilung 2022-02

Schwachstelle im Spring-Framework (CVE-2022-22965)

Stand: 05.04.2022 – 15:00 Uhr

Am Mittwoch, den 30.03.2022 haben Gerüchte über eine 0Day-Schwachstelle in Spring Framework, einem Framework zur Entwicklung von Java-Anwendungen, die Runde gemacht. Aufgrund der Verbreitung von Spring Framework wurden schnell Vergleiche mit der Schwachstelle Log4Shell (CVE-2021-44228) gezogen, die Ende 2021 die Sicherheitsbeauftragten weltweit in Atem gehalten hat.

Quelle: DFN – Deutsches Forschungsnetz
https://www.dfn-cert.de/aktuell/0day-schwachstelle-spring-framework-apache-tomcat-CVE-2022-22965.html

Eine Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) existiert hierzu nach unserer Kenntnis nicht.

Offizielle Informationen zur Schwachstelle wurden von VMware Inc., Eigentümerin des Spring Frameworks, am 31.03.2022 veröffentlicht: https://tanzu.vmware.com/security/cve-2022-22965

Danach besteht ein Sicherheits-Risiko nur beim Vorliegen der folgenden Voraussetzungen:

- Einsatz der Software unter Apache Tomcat als Servlet Container
  Hierzu hat Apache Tomcat mittlerweile die Versionen 10.0.20, 9.0.62 and 8.5.78 veröffentlicht, die eine Ausnutzung der Schwachstelle unterbinden
- Software-Paketierung als WAR-File
- Einsatz der Java-Version 9 (JDK 9) oder höher
- Nutzung von Spring MVC oder Spring WebFlux in bestimmten Versionen

Welche Lösungen von hallobtf! können betroffen sein?

Da ausschließlich die Software Kai die Möglichkeit vorsieht, die Server-Komponente unter Apache Tomcat zu betreiben, **sind alle anderen hallobtf! Software-Lösungen von der Schwachstelle per se nicht betroffen**.

Kai kann ausschließlich dann betroffen sein, wenn der Kai-Server unter Apache Tomcat betrieben wird.

Welche Empfehlungen gibt hallobtf!?

Sofern der Kai-Server unter Apache Tomcat betrieben wird, wird empfohlen, die genannten Voraussetzungen zu prüfen und die Betriebs-Umgebung gegebenenfalls anzupassen.