Service-Mitteilung 2021-02

Kritische Schwachstelle in Log4j

Stand: 16.12.2021 – 15:00 Uhr

Diese Service-Mitteilung betrifft die kommunalen Lösungen *Doppik al dente!*®, PTV und javaPrint. Für die Inventarisierungslösung Kai wird auf die Service-Mitteilung 2021-01 verwiesen.

Update 21.12.2021 – 14:00 Uhr

Mittlerweile werden in der Fachwelt Denial-of-Service (Dos)-Schwachstellen diskutiert, die Log4j bis inklusive Version 2.16.0 betreffen. Hierbei geht es jedoch nicht um die Einschleusung und Ausführung von schädlichem Programmcode sondern um die (theoretische) Möglichkeit, dass die Anwendung in unendliche Rekursionsschleifen gerät und dadurch letztendlich zum Erliegen kommt.

Da die kommunalen Lösungen von hallobtf! – anders als beispielsweise Applikationen zur Prozess-Steuerung – keinen kritischen Hochverfügbarkeitsanforderungen unterliegen, ergibt sich hieraus unseres Erachtens keine besondere Bedrohungslage. Unsere Analysen ergaben darüber hinaus, dass eine entsprechende Konstellation nahezu ausgeschlossen werden kann.

Auch das BSI hat hierzu keine weiteren Empfehlungen herausgegeben. Wir haben daher darauf verzichtet, erneut Versionen unserer Softwareprodukte bereitzustellen, die die tagesgenau aktuelle Version von log4j (derzeit 2.17) enthalten.

Wir beobachten jedoch täglich die aktuelle Entwicklung und werden beim Bekanntwerden neuer Bedrohungsszenarien unverzüglich reagieren.

Am 9. Dezember 2021 wurde in der weit verbreiteten JAVA-Bibliothek **log4j** eine Sicherheitslücke entdeckt und unter dem Stichwort "Log4Shell" mit der Nummer CVE-2021-44228 registriert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gab hierzu eine Cyber-Sicherheitswarnung heraus, die unter der CSW-Nummer 2021-549032-1432 aktuell in der Version 1.4 vom 13.12.2021 vorliegt. Sie wurde ergänzt durch eine weitere Cyber-Sicherheitswarnung unter der CSW-Nummer 2021-549177-1032, die aktuell in der Version 1.0 vom 14.12.2021 vorliegt.

Die Bedrohungslage wurde vom BSI als "rot" (extrem kritisch) eingestuft.

Worin besteht die Sicherheitslücke?

Die log4j-Bibliothek wird in der Java-Welt häufig für das Management der von einer Anwendung erzeugten Protokoll-Daten genutzt. Auch einige Lösungen von hallobtf! nutzen die log4j-Bibliothek für diesen Zweck.

Seit der Version 2.0 verfügt log4j über eine Komponente JndiLookup, die die zu protokollierenden Daten "ausführt". Werden nun Daten protokolliert, die "zufälligerweise" bestimmte Programmbefehle enthalten, so werden diese Programmbefehle durch die Komponente JndiLookup ausgeführt. Ein (externer oder interner) Nutzer der betreffenden Anwendung kann diese somit möglicherweise veranlassen, nahezu beliebigen (schädlichen) Programmcode auszuführen.

Die log4j-Versionen 1.x enthalten die JndiLookup-Komponente nicht und können daher in dieser Hinsicht als sicher gelten. Das BSI weist jedoch darauf hin, dass sie nicht mehr vom Hersteller unterstützt werden und (daher vermutlich) diverse andere Schwachstellen aufweisen.

Kommunale Lösungen von hallobtf!
Service-Mitteilung 2021-02: kritische Schwachstelle in Log4j

Welche Lösungen von hallobtf! nutzen die log4j-Bibliothek?

Die kommunalen Lösungen von hallobtf! nutzen unterschiedliche Versionen der log4j-Bibliothek:

- ***Doppik al dente!*® (DaD)** nutzt die log4j-Bibliothek in der Version 1.2.

  Von daher besteht hinsichtlich der aktuellen Schwachstelle in der log4j-Bibliothek keine Gefahr. Jedoch sollte entsprechend den Empfehlungen des BSI bei nächster Gelegenheit ein Update erfolgen.

  Auf der *Doppik al dente!*® -Webseite (www.doppik-al-dente.de) steht die DaD-Version 02.02 r18185 zum Download bereit. Diese enthält die log4j-Bibliothek in der Version 2.16, in der (nach dem derzeitigen Erkenntnisstand) die Sicherheitslücke geschlossen ist.

  Wichtiger Hinweis: *Bitte kontaktieren Sie uns, wenn Sie das "DaD-Schwesterprodukt" Doppik al dente!® - Konzernreporting nutzen und auf einen neuen Stand mit der log4j-Bibliothek in der Version 2.16 upgraden möchten.*

- Ältere Versionen von **PTV** nutzen die log4j-Bibliothek nicht. In neueren kommt die log4j-Biliothek in der Version 2.13 zum Einsatz.

  Es steht eine PTV-Version 05.05 r18185 zur Verfügung. Diese enthält die log4j-Bibliothek in der Version 2.16, in der (nach dem derzeitigen Erkenntnisstand) die Sicherheitslücke geschlossen ist.

  Bitte kontaktieren Sie uns, wenn Sie PTV upgraden möchten.

- In **javaPrint** kommt die log4j-Bibliothek nicht zum Einsatz. Es besteht daher kein aktueller Handlungsbedarf.