Service-Mitteilung 2021-01

Kritische Schwachstelle in Log4j

Stand: 16.12.2021 – 15:00 Uhr

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 Kai – anders als beispielsweise Applikationen zur Prozess-Steuerung – keinen kritischen Hochverfügbarkeitsanforderungen unterliegt, 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 eine Version von Kai bereitzustellen, die die tagesgenau aktuelle Version von log4j (derzeit 2.17) enthält.

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 Kai nutzt 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.

Kann die Sicherheitslücke auf einfache Weise geschlossen werden?

Die log4j-Bibliothek bietet die Möglichkeit, die JndiLookup-Komponente durch einen Installationsschalter

```
log4j2.formatMsgNoLookups=true
```

zu deaktivieren. Allerdings besteht diese Möglichkeit erst ab der log4j-Version 2.10 und es ist in der Fachwelt durchaus umstritten, ob damit ein wirklich sicherer Schutz erreicht werden kann.

Das BSI empfiehlt den Einsatz dieses Schalters als "Mitigationsmaßnahme" zur Verminderung des Risikos in all den Fällen, in denen nicht kurzfristig auf eine neue, sichere Version der Software umgestellt werden kann.

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.

Nutzt Kai die log4j-Bibliothek?

Ja. Kai nutzt die log4j-Bibliothek zur Aggregation der von den einzelnen Kai-Komponenten erzeugten Protokoll-Daten.

Je nach der installierten Kai-Version kommen unterschiedliche Versionen der log4j-Bibliothek zum Einsatz:

- Die Kai-Version 02.02 nutzt log4j in der Version 1.2
- Die Kai-Version 02.03 nutzt (bisher) log4j in der Version 2.12 oder 2.13

Eine genaue Analyse der Datenprotokollierung in Kai ergab jedoch, dass mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann, dass es in Kai durch die Nutzung der log4j-Bibliothek zur Ausführung von irgendwelchem (schädlichen) Programmcode kommen kann.

Eine 100%ige Garantie hierfür kann jedoch nicht gegeben werden.

Gibt es eine Version von Kai, in der die Sicherheitslücke geschlossen ist?

Ja. Auf der Kai-Webseite (www.hallokai.de) steht die Kai-Version 02.03 r18184 zum Download bereit.

Diese enthält die log4j-Bibliothek in der Version 2.16. In dieser ist (nach dem derzeitigen Erkenntnisstand) die Sicherheitslücke geschlossen.

Wo kann ich den Installationsschalter setzen?

Das BSI empfiehlt den Einsatz des Installations-Schalters (siehe oben) nur in den Fällen, in denen nicht kurzfristig auf eine neue, sichere Version der Software umgestellt werden kann, als Maßnahme zur Verminderung des Risikos.

Dieser ist in den Dateien

- server\custom\Server.ini
- client\custom\Client.ini
- laptop\custom\Laptop.ini

in der Rubrik [SYSTEMPROPERTIES] zu setzen.

```
[SYSTEMPROPERTIES]
log4j2.formatMsgNoLookups=true
```