Niedersächsisches Landesamt
für Bau und Liegenschaften

LISA
Liegenschaftsinformationssystem
Außenanlagen

Dezember 2022

Wichtige Informationen zur Kritische Schwachstelle in der Java-Bibliothek log4j

Log4j-Schwachstelle

Ansätze zur Schließung der Lücke

Herausgeber und Redaktion
Leitstelle des Bundes für Liegenschaftsbestandsdokumentation
Niedersächsisches Landesamt für Bau und Liegenschaften
Referat BL 15
Postfach 240
30002 Hannover

Inhalt

Tabelle 1: Dokumentversion

Dokumentversion	Bemerkung
Version 2	05.12.2022

1 Einleitung

Eine kritische Schwachstelle in der weit verbreiteten Java-Bibliothek Log4j, die als Log4Shell bezeichnet wird, führt nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer sehr kritischen Bedrohungslage.

Auch Produkte des Liegenschaftsinformationssystems für Außenanlagen des Bundes LISA sind von der Schwachstelle in Log4j betroffen.

2 Betroffene Produkte

- GIS Portal der Firma VertiGIS (vormals AED-SICAD)
- ArcGIS der Firma ESRI
- Oracle DBMS und Oracle Client
- LISA Migration

Die Softwareprodukte sind Grundlage für die LISA Web-Auskunft und den LISA LM Server.

Alle weiteren Produkte des LISA sind nach jetzigen Erkenntnissen nicht von der Schwachstelle betroffen. Auch nicht die in Java entwickelten Produkte INSA und ADMIN.

Bitte führen Sie für die betroffenen Produkte auf den entsprechenden Rechnern die in den folgenden Kapiteln beschriebenen Aktionen durch
Bei Fragen und Problemen werden Sie sich entweder an den Support der Firma VertiGIS (support@vertigis.zendesk.com) oder den LISA Support (support-lisa@nlbl.niedersachsen.de).

3 GIS Portal (LISA Web-Auskunft)

Die Software ist auf Ihrem Web-Server für die LISA Auskunft installiert. Dort ist zudem ein Apache Tomcat in Betrieb. Gehen Sie folgendermaßen vor:

1. Laden Sie die Log4j-Dateien Verion 2.18.0 runter
   (z.B. hier: Maven Repository: org.apache.logging.log4j » log4j (mvnrepository.com))
2. Stoppen Sie den Apache Tomcat (über den entsprechenden Dienst).
3. Wechseln Sie in einem Datei Explorer in das Verzeichnis „webapps“ Ihrer Tomcat-Installation. In diesem Verzeichnis finden Sie die installierten Web-Anwendungen als Unterverzeichnisse. Für die nächsten Schritte sind folgende Verzeichnisse relevant:
   - ASmobile
   - ASWeb
   - ASWebURM
4. Führen Sie für alle oben genannten Unterverzeichnisse, sofern sie sich in Ihrem webapps-Verzeichnis befinden, die folgenden Schritte durch:
   a. Wechseln Sie in das Verzeichnis und dort in das Unterverzeichnis „WEB-INF\lib“.
   b. Ersetzen Sie dort die folgenden Dateien – falls vorhanden – durch die entsprechenden mitgelieferten Dateien, indem Sie die vorhandenen Dateien löschen und die neuen Dateien in das Verzeichnis kopieren:
      log4j-core-2.XX.XX.jar durch log4j-core-2.18.0.jar
      log4j-api-2. XX.XX.jar durch log4j-api-2.18.0.jar
      log4j-web-2.XX.XX.jar durch log4j-web-2.18.0.jar
      log4j-1.2-api-2.XX.XX..jar durch log4j-1.2-api-2.18.0.jar
5. Starten Sie den Apache Tomcat neu.
6. Prüfen Sie, ob die LISA Web-Auskunft noch einwandfrei läuft.

4 ArcGIS Server

ArcGIS 10.7.1 und frühere Versionen sind potenziell gefährdet, und es laufen derzeit weitere Analysen bei Esri Inc., um die Angreifbarkeit zu ermitteln. CVE-2021-44228 kann in ArcGIS Enterprise 10.8 und höher nicht ausgenutzt werden. Im Bereich LISA ist zurzeit nur die Nutzung der Versionen 10.6.1 und 10.7.1 möglich. Die Option eines Upgrades entfällt daher. Es wird dringend empfohlen für gefährdete Systeme sofort umfassende Abwehrmaßnahmen zu ergreifen.

Aktuelle Informationen finden Sie hier:

https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/

Es liegt nun ein Patch zum Schließen der Lücke für ArcGIS Server 10.6.1 und 10.7.1 vor.

1. Laden Sie aktuellsten Patch herunter.
   Für ArcGIS Server 10.6.1: https://support.esri.com/en/download/7966
   Für ArcGIS Server 10.7.1: https://support.esri.com/en/download/7975
2. Installieren Sie entsprechend den Hinweise auf den oben genannten Internetseiten.

Weitere Informationen: https://support.esri.com/en/Technical-Article/000026951

5 Oracle 19c

In den Systemvoraussetzungen des LM wird als Voraussetzung die Version 19.3 für das Oracle DBMS angegeben. Neben Performanz-Problemen in Zusammenhang mit LISA enthält diese Version noch indirekt Sicherheitslücken bzgl. log4j:

Die Ordner beinhalten noch diverse log4j-Dateien, die offiziell nicht verwendet werden. Sind Reste aus Oracle 11 und 12, die nicht gelöscht wurden sind beim Zusammenstellen der Version 19.3. Ab Update Release 19.12 sind die betreffenden Dateien gelöscht bzw. bei Notwendigkeit mit neueren Versionen ersetzt worden[1]. Letztmalig nahm Oracle explizit Bezug auf das Problem bei Release 19.14[2].
Da auch Probleme mit der Performanz in dieser Version bestehen, empfehlen wir dringend auf die Version 19.16 zu aktualisieren. Diese wurde auch von VertiGIS noch einmal getestet und für das LM freigegeben. Ein entsprechender Leitfaden zum Umstieg steht auf www.lisa-bund.de bereit.

6 LISA Migration

Die LISA Migration nutzt die FME 2018 für die Migration der Daten aus dem ALK-GIAP. Für dieses Produkt wird vom Softwarehersteller (Safe Software) kein Patch mehr bereit gestellt, der die Log4j-Sicherheitslücke schließt.

Um die Software weiterhin nutzen zu können, sind daher folgende Dateien aus dem Installationsverzeichnis der FME 2018 (z.B. „C:\FME“) zu löschen:

<Installationsverzeichnis FME>\plugins\activemq-all-5.6.0.jar

<Installationsverzeichnis FME>\plugins\log4j-1.2.16.jar

Die LISA Migration arbeitet auch nach dem Löschen der Dateien weiterhin fehlerfrei.

[1] Document 2828303.1 (oracle.com)
[2] Document 2828594.1 (oracle.com)