ecatDesigner und log4j Info (CVE-2021-44228)

1.1 Webapplikation

- Der ecatDesigner benutzt das log4j Framework **NICHT** für eigene Logfiles

1.2 Webserver

- Der Tomcat Server benutzt das log4j Framework **NICHT** für internes Logging

The internal logging for Apache Tomcat uses JULI, a packaged renamed fork of Apache Commons Logging that, by default, is hard-coded to use the java.util.logging framework. This ensures that Tomcat's internal logging and any web application logging will remain independent, even if a web application uses Apache Commons Logging.

1.3 Java Abhängigkeiten

- Der ecatDESIGNER hat Abhängigkeiten die log4j mit aufgenommen haben
  - Diese Abhängigkeit ist vorhanden ab **Version 4987**
  - Es wird **log4j 2.13.3** eingebunden
- Die Abhängigkeiten sind für zukünftige Entwicklungen aufgenommen worden und haben momentan **keinen** aktiven Teil innerhalb der Applikation

1.4 Sicherheitsmaßnahmen

- semaino wird die Abhängigkeit in neueren Version entfernen
- Für bestehende Installationen empfehlen wir folgende Vorgehensweise:
  - Für die log4j Versionen >=2.10 kann der JNDI Lookup per ENV-Variable deaktiviert werden

    -DLOG4J_FORMAT_MSG_NO_LOOKUPS=**true**
  - Zusätzlich kann die fehlerhafte Klasse entfernt werden:
    - Im Ordner .../ECATHOME/ecatDESIGNER/WEB-INF/lib die Datei **log4j-core-2.13.3.jar** öffnen (mit z.B. 7zip)
    - in den Pfad /org/apache/logging/log4j/core/lookup/ navigieren
    - die Datei JndiLookup.class löschen

1.5 Links

1. Tomcat Logging: https://tomcat.apache.org/tomcat-8.0-doc/logging.html
2. Log4j Security: https://logging.apache.org/log4j/2.x/security.html
3. Ausführungen des BSI: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3
4. 7zip: https://www.7-zip.dee