log4j JNDI Vulnerability

Vor dem Löschen oder Ausführen von Operationen ein Backup des Tomcat-Verzeichnisses vornehmen!

Verwundbare Libraries selbst auffinden

externes Tool von Github: https://github.com/mergebase/log4j-detector

```
wget https://github.com/edu-sharing/log4j-detector/raw/master/log4j-detector-2021.12.13.jar

java -jar log4j-detector-2021.12.13.jar /opt/alfresco-community/tomcat
```

Only versions of Log4J 2.x (from 2.0-beta9 to 2.14.1) are vulnerable to CVE-2021-44228.

edu-sharing <= 5.0

Kein log4j 2.x, aktuell nicht von CVE-2021-44228 betroffen

edu-sharing 5.1

Betroffene Libraries:

- edu-sharing/WEB-INF/lib/edu_sharing-elasticsearch-1.0.jar

```
zip -q -d /opt/alfresco-community/tomcat/webapps/edu-sharing/WEB-INF/lib/edu_sharing-elasticsearch-1.0.jar org
/apache/logging/log4j/core/lookup/JndiLookup.class
```

Nach dem Löschen der Klassen den gesamten Tomcat/Alfresco neustarten

edu-sharing 6.0

Kein log4j 2.x, aktuell nicht von CVE-2021-44228 betroffen

Sofern Elasticsearch im Einsatz: Elasticsearch-Server auf Verwundbarkeit prüfen!

Überprüfung einzelner Komponenten/Abhängigkeiten

- alfresco: log4j-1.2.17.jar (Nicht verwundbar)
- solr 4: log4j-1.2.17.jar (Nicht verwundbar)
- edu-sharing: log4j-1.2.8.jar (Nicht verwundbar)
- spring-boot (tracker,escm): nutzt kein log4 core (Nicht verwundbar)
- Elasticsearch-Tracker: (Nicht verwundbar)

Elasticsearch Server:

Siehe https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476