Log4j-Sicherheitslücke (CVE-2021-44228)

Eine Sicherheitslücke in der Java-Bibliothek Log4j gefährdet aktuell Millionen von Onlineanwendungen weltweit. Die Schwachstelle CVE-2021-44228 für die Protokollierung von Ereignissen kann zur Remote-Ausführung von Code durch Dritte führen.

Von ELO entwickelte Dienste, die u. a. unsere öffentliche API bereitstellen und potenziell im Internet verfügbar sind, **setzen Log4j in der Version 2 nicht ein** und sind somit von der Schwachstelle **nicht betroffen**. Leider ist jedoch unsere aktuelle ElasticSearch-Version (ab ELO 10), der ELO Java Client (ab ELO 10) sowie ELO BLP in Version 5.2 **potenziell betroffen**.

Sicherheitsexperten weltweit arbeiten gerade mit Hochdruck an der Analyse weiterer Auswirkungen. Wir empfehlen daher, **auf die von uns bereitgestellten Versionen zu aktualisieren** und unsere **Handlungsempfehlungen umzusetzen**. Unsere ELO Entwicklung hat mögliche Auswirkungen für die ELO Systeme intensiv analysiert und stellt Ihnen neue ELO Java Clients zur Verfügung, die die Sicherheitslücke schließen. Diese stehen hier für Sie zum Download bereit:

Java Client 21.01.002: https://download.elo.com/PSupport/Support/Javaclients/ELO21/JC_X64_21_01_002_96.zip
Java Client 20.07.003: https://download.elo.com/PSupport/Support/Javaclients/ELO20/JC_X64_20_07_003_190.zip
Java Client 12.11.002: https://download.elo.com/PSupport/Support/Javaclients/ELO12/JC_X64_12_11_002_269.zip
Java Client 11.13.002: https://download.elo.com/PSupport/Support/Javaclients/ELO11/JC_X86_11_13_002_173.zip
Java Client 10.17.001: https://download.elo.com/PSupport/Support/Javaclients/ELO10/JC_X86zulu_10_17_001_286.zip
Java Client 10.17.001: https://download.elo.com/PSupport/Support/Javaclients/ELO10/JC_X64zulu_10_17_001_286.zip

In diesem Zuge ist es auch wichtig, die ELO iSearch zu aktualisieren. Hier die konkreten Handlungsempfehlungen für die ELO iSearch:

Die ELO iSearch nutzt log4j in Version 2.9.1. Wir empfehlen, die verwendeten log4j-Bibliotheken durch die der Version 2.16.0 auszutauschen.

Update der Libraries unter Windows:

Unter Windows hilft Ihnen folgende Kurzbeschreibung, um die Sicherheitslücke zu schließen.

Bitte:

- Den Dienst ELO-servername-iSearch stoppen.
- Löschen Sie die 3 Dateien im Verzeichnis /instdir/servers/ELO-servername-iSearch/lib

  log4j-1.2-api-2.9.1.jar
  log4j-api-2.9.1.jar
  log4j-core-2.9.1.jar

- Download von Apache Log4j 2.16.0
- https://logging.apache.org/log4j/2.x/download.html
- Kopieren Sie die drei Dateien:

  log4j-1.2-api-2.16.0.jar
  log4j-api-2.16.0.jar

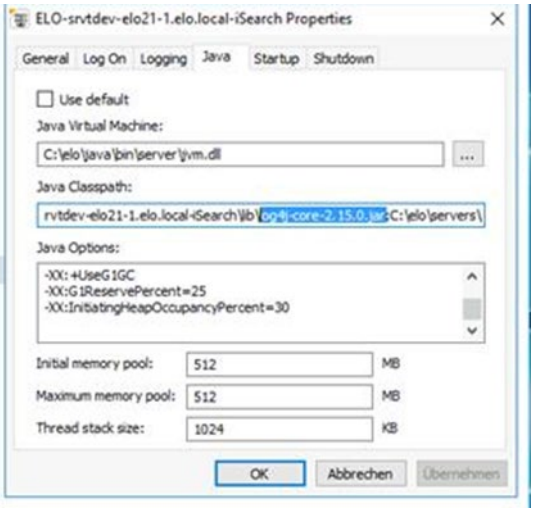
log4j-core-2.16.0.jar

nach (Beispiel):
C:\ELO\servers\ELO-servername-iSearch\lib\

- Starten Sie die ELO-servername-iSearchw.exe. Diese befindet sich in der ELO Standardinstallation unter (Beispiel):

  C:\ELO\servers\ELO-servername-iSearch\bin\ELO-servername-iSearchw.exe
  um die Konfiguration anzupassen.

- Ersetzen Sie die 3 alten log4j-jars im Java class path der Konfiguration des iSearch-Services (3 Dateien)



  Statt bisher:
  log4j-1.2-api-2.9.1.jar
  log4j-api-2.9.1.jar
  log4j-core-2.9.1.jar
  sind in der Zeile die Werte:
  log4j-1.2-api-2.16.0.jar
  log4j-api-2.16.0.jar
  log4j-core-2.16.0.jar
  einzutragen. Die Zeile ist sehr lang. Es empfiehlt sich daher, die ganze Zeile in einen einfachen Editor wie Notepad zu kopieren, dort zu bearbeiten und zu prüfen, bevor diese in der Eingabezeile des Konfigurationsprogramms angepasst wird.

- Den Dienst ELO-servername-iSearch wieder starten.

In diesem Zusammenhang ist es ebenfalls sinnvoll, den **Indexserver** auf die neueste Version zu aktualisieren, da diese zusätzliche Sicherheitsverbesserungen enthält (unabhängig von log4j). Sollten Sie den **ELO BLP in der Version 5.2** im Einsatz haben, sind zusätzliche Schritte erforderlich. **Bitte kontaktieren Sie hierfür Ihren ELO Business Partner.**

Damit haben Sie Ihr ELO System gegen die **Log4j-Sicherheitslücke (CVE-2021-44228) erfolgreich geschützt.**