To all ELO customers

Regarding the zero-day exploit in Log4J / CVE-2021-44228 – Log4j 2 vulnerability

A recently discovered **security gap in the Java library Log4j** is putting millions of online applications at risk worldwide. The vulnerability CVE-2021-44228 for logging events could lead to third parties executing remote code.

Services developed by ELO that among other things provide our public API and may be available online do not use version 2 of Log4j and therefore are **not affected.** However, our current Elasticsearch version (from ELO 10), the ELO Java Client (from ELO 10), and version 5.2 of ELO BLP unfortunately **are affected.**

Safety experts worldwide are working at full speed to analyze further effects of this vulnerability. We therefore recommend updating to the versions provided by us and implementing our recommended actions. Our ELO Development department has analyzed the effects for our systems in detail and has made new ELO Java Client versions that close the security gap available. You can download them here:

Java Client 21.01.002: https://download.elo.com/PSupport/Support/Javaclients/ELO21/JC_X64_21_01_002_96.zip
Java Client 20.07.002: https://download.elo.com/PSupport/Support/Javaclients/ELO20/JC_X64_20_07_002_188.zip
Java Client 12.11.001: https://download.elo.com/PSupport/Support/Javaclients/ELO12/JC_X64_12_11_001_268.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 order to protect your systems, it is also important to update the ELO iSearch. Below you will find the specific recommended actions for ELO iSearch:

ELO iSearch uses version 2.9.1 of Log4j. We recommend replacing the Log4j libraries in use with the version 2.16.0.

Updating the libraries on Windows:

The following brief instructions will help you close the gap in Windows systems.

Please:

- Stop the ELO-servername-iSearch service
- Delete the 3 files in the directory /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 Apache Log4j 2.16.0
- https://logging.apache.org/log4j/2.x/download.html

- Copy the three files:

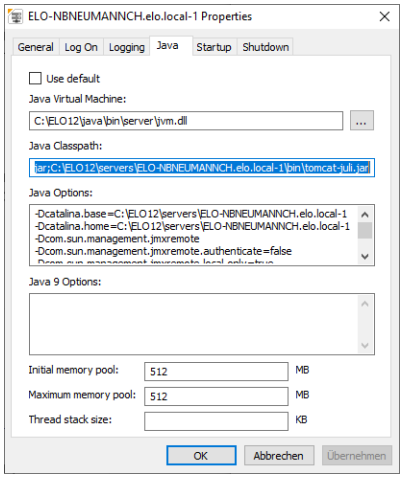
  `log4j-1.2-api-2.16.0.jar`
  `log4j-api-2.16.0.jar`
  `log4j-core-2.16.0.jar`

  to (example):

  C:\ELO\servers\ELO-servername-iSearch\lib\
- Start ELO-servername-iSearchw.exe. In standard ELO installations, this is located at (example):

  C:\ELO\servers\ELO-servername-iSearch\bin\ELO-servername-iSearchw.exe

  to modify the configuration.
- Replace the 3 old log4j-jars in the Java class path of the iSearch service configuration (3 files)



  Instead of the previous:

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

  enter the following values in the line:

  `log4j-1.2-api-2.16.0.jar`
  `log4j-api-2.16.0.jar`
  `log4j-core-2.16.0.jar`

  The line is very long. We recommend copying the entire line to a simple editor such as Notepad and to edit and check it there before modifying it in the configuration program's input line.
- Start the ELO-servername-iSearch service

In this context, it also makes sense to update the Indexserver to the latest release which contains additional security improvements (not related to log4j). If you're running BLP version 5.2 additional steps are required. Please contact your ELO Business Partner to this end.

You have then successfully protected your ELO system against the CVE-2021-44228 – Log4j 2 vulnerability.