SICHERHEIT

Guide zur Log4j-Schwachstelle

Stand: 18.03.2021

Sehr geehrte Kundin, sehr geehrter Kunde,

Aufgrund der aktuellen Bedrohung von IT-Systemen durch die Sicherheitslücke im Programmschnipsel log4j möchten wir Ihnen mit diesem Dokument Informationen und Hilfestellungen an die Hand geben.

Leider ist auch ELO betroffen. Potentiell gefährdet ist die aktuelle ElasticSearch-Version und der ELO Java Client – ab ELO 10.

Die von ELO entwickelten Dienste, die u. a. die öffentliche API bereitstellen und potentiell im Internet verfügbar sind, setzen log4j in der Version 2 nicht ein und sind somit nicht betroffen.

SideStep-Lösungen, wie beispielsweise die SiConnect, sind von der Sicherheitslücke nicht betroffen.

AKTUELLES

Verwundbarkeiten in log4j2 2.16.0 und 2.17.0

Aussage des Herstellers

log4j2 befindet sich seit dem ersten veröffentlichten Sicherheitsproblem nun verstärkt unter Beobachtung. Es ist durchaus wahrscheinlich, dass in den kommenden Wochen weitere Lücken gefunden werden. Derzeit sind zwei weitere bekannt. In CVE-2021-44832 (verwundbare Version bis 2.17.0) ist festgehalten, dass eine Remote Code Execution (RCE) möglich ist, wenn ein JDBC Appender konfiguriert ist, der eine JNDI Datasource verwendet.

CVE-2021-45105 (verwundbare Version bis 2.16.0) beschreibt ein Denial of Service (DoS), wenn in der Konfiguration Context-Lookups (bsp.: ${ctx:...}) verwendet werden.

- Beide Probleme sind in der Version 2.17.1 von log4j2 behoben.
- In kommenden Veröffentlichungen von ELO Modulen wird ELO auf diese Version aktualisieren.

Derzeit besteht kein zwingender Handlungsbedarf zum Upgrade, solange die Voraussetzungen zum Ausnutzen der Probleme nicht erfüllt sind!

In einer ELO Standardinstallation können sie nicht ausgenutzt werden, da die Logging-Konfiguration weder einen JDBC Appender noch Context-Lookups verwendet.

ALLGEMEINER HINWEIS

Allgemeine Empfehlung

Prüfen Sie zunächst die Bereitstellung von Systemfunktionen nach außen:
Ist Ihr ELO-System von extern erreichbar? Nur dann ist die Ausnutzung der Schwachstelle von extern möglich.

Alle aus dem Internet erreichbaren Anwendungen (JAVA), die anhand von log4j protokollieren, können potentiell betroffen sein. Deaktivieren Sie entsprechende Dienste sobald wie möglich.

Wurde bereits eine andere Sicherheitslücke ausgenutzt und das interne Netz kompromittiert, ist eine weitere Ausnutzung dieser Sicherheitslücke von intern noch nicht auszuschließen. Eine finale Aussage wurde hierzu von Seiten des Herstellers, der ELO Digital Office GmbH, allerdings noch nicht getroffen.

___

Auf den nachfolgenden Seiten finden Sie weitere Informationen und Handlungsempfehlungen, welche uns zum aktuellen Zeitpunkt von Seiten des Herstellers zur Verfügung stehen.

SICHERHEIT

Überblick

Betroffene Komponenten

Folgende Komponenten sind von der Sicherheitslücke Log4j betroffen – setzen eine ältere Java Version ein (welche eine Remote Code Execution zulässt) und sollten umgehend aktualisiert werden:

Java Clients

Aktualisieren der Java Clients für Versionen 10, 11, 12, 20, 21.

ElasticSearch

Aktualisieren von ElasticSearch mithilfe des Server Setups. Hierbei wird ebenfalls eine aktuelle Indexserver Version verteilt.

Nicht gefährdete Komponenten

ELO Business Solutions

Die Business Solutions sowie das ELO Job Portal von ELO HR Recruiting sind hiervon nicht betroffen da log4j2 nicht zum Einsatz kommt.

Allgemeine Dienste

Grundlegend sind ELO Kern-Dienste von der Schwachstelle nicht betroffen, da log4j 2.x in den zentralen Diensten, welche u.a. eine öffentliche API zur Verfügung stellen, keine Anwendung findet. Dies betrifft u.a.:

- ELO Indexserver
- ELO Web Client
- ELO WF
- ELO Admin Console
- ELO Automation Services
- ELO Fulltext und Textreader
- ELO Teamroom
- ELO Replikation
- ELO Importer

Einige ELO Dienste enthalten eine log4j2 API-Bibliothek und sind als unkritisch einzustufen. Betroffen ist nur die eigentliche Implementierung des Logging-Frameworks aus der log4j2-Core-Bibliothek welche in den folgenden Diensten nicht enthalten ist.

- ELO IMO
- ELO Rest
- ELO Smart Input

Die SideStep-Lösungen

Die von Ihnen erworbenen SideStep-Lösungen, wie beispielsweise die SiConnect, enthalten keine Log4j-Anwendungen. Sie sind somit von der Sicherheitslücke nicht betroffen.

TECHNISCH

Konkrete Handlungsempfehlungen

Java Client

Der Java Client verwendet für das Logging ab ELO 10 Log4j2. Ein Update des Java Clients auf aktuelle Versionen wird empfohlen. Aktuell verfügbare Versionen enthalten eine aktuelle Version von log4j 2.16.0.

Betroffene Versionen und Links zum Download von Informationen und Installationspaketen zum Update:

Java Client 21.01.002 (64 Bit):
https://download.elo.com/PSupport/Support/Javaclients/ELO21/JC_X64_21_01_002_96.zip

Java Client 20.07.003 (64 Bit):
https://download.elo.com/PSupport/Support/Javaclients/ELO20/JC_X64_20_07_003_190.zip

Java Client 12.11.002 (64 Bit):
https://download.elo.com/PSupport/Support/Javaclients/ELO12/JC_X64_12_11_002_269.zip

Java Client 11.13.002 (32 Bit):
https://download.elo.com/PSupport/Support/Javaclients/ELO11/JC_X86_11_13_002_173.zip

Java Client 10.17.001 (32 Bit):
https://download.elo.com/PSupport/Support/Javaclients/ELO10/JC_X86zulu_10_17_001_286.zip

Java Client 10.17.001 (64 Bit):
https://download.elo.com/PSupport/Support/Javaclients/ELO10/JC_X64zulu_10_17_001_286.zip

Nicht betroffen, kein Einsatz von log4j2:

- Java Client 9

Java Client bis einschließlich 11.05, enthält ein Java 8u172, Java Client bis einschließlich 10.10, enthält ein Java 8u172. Diese Versionen setzen noch ältere Java Versionen ein, bei denen eine Remote Code Execution über JNDI-ldap-Aufrufe vollumfänglich möglich sind.

ElasticSearch

Basisinformationen

ElasticSearch setzt standardmäßig log4j2 für das Logging ein und stellt somit ein potentielles Risiko dar. Uns war es bisher nicht möglich die Schwachstelle über gezielte Angriffe, bspw. die ELO Suche oder direkte Authentifizierung über SearchGuard zu nutzen. Es werden bspw. keine Queries protokolliert, sodass Sucheingaben im Client nicht im Log ausgegeben werden. Günstig für das Verhindern möglicher Angriffsszenarien ist zudem, dass der Index Server, welcher nicht von der Sicherheitslücke betroffen ist Anfragen entgegennimmt und an die ElasticSearch weiterleitet.
Wir empfehlen ein Update über ein neues Serversetup.

Betroffene Versionen sind u.a.:

- ElasticSearch Installationen durch das Serversetup ELO 10
- ElasticSearch Installationen durch das Serversetup ELO 11
- ElasticSearch Installationen durch das Serversetup ELO 12
- ElasticSearch Installationen durch das Serversetup ELO 20
- ElasticSearch Installationen durch das Serversetup ELO 21

ElasticSearch Versionen in ELO 12, 20 sowie 21 enthalten eine neuere Java Version die eine Remote Code Execution über JNDI-ldap-Aufrufe verhindert. Dies wird aber nicht als ausreichender Schutz angesehen.

Empfehlung

ELO ElasticSearch nutzt die Version 2.9.1 von Log4j. Die Log4j Bibliotheken sollten durch Version 2.16.0 ersetzt werden.

Update der Bibliothek unter Windows

Folgen Sie der Anleitung, um ein Update durchzuführen.

- Dienst ELO-servername-iSearch stoppen
- Löschen der 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 dieser der 3 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 ELO-servername-iSearchw.exe., um die Konfiguration zu modifizieren.
  In Standardinstallationen hier zu finden (Beispiel):
  C:\ELO\servers\ELO-servername-iSearch\bin\ELO-servername-iSearchw.exe
- Ersetzen Sie die 3 alten log4j-jars im Pfad der JAVA Klasse der Service-Konfiguration der ElasticSearch.

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

Statt der Folgenden:
Tragen Sie diese Werte in die Zeile ein:

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

Die Zeile ist sehr lang. Wir empfehlen die gesamte Zeile zunächst in einen einfachen Editor (wie Notepad) und die Prüfung und Anpassungen hier vorzunehmen.

- Dienst ELO-servername-iSearch starten

ALLGEMEIN

Weitere Empfehlung

Unabhängig von der Sicherheitslücke Log4j

ELO empfiehlt darüber hinaus die bereitgestellten Indexserver Versionen einzuspielen, welche, unabhängig von der Sicherheitslücke Log4j, einige aktuelle Sicherheitsupdates zum Schutz der ELO Systeme enthalten. Diese Versionen sind Teil der neuen Server Setups.

- ELO IX 11.05.003
- ELO IX 12.07.005
- ELO IX 21.01.001