1 Log4j (GERMAN v.1.2 – 17.12.21)

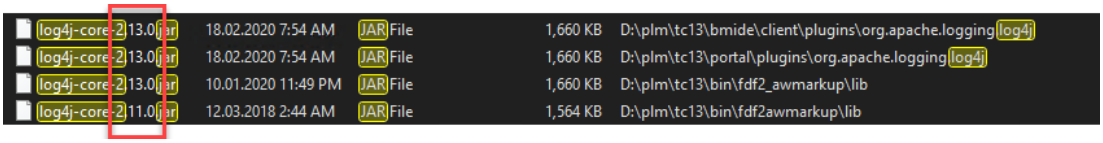
Es gibt eine kritische Sicherheitslücke im open Source Modul **log4j**, welches von Java für Logfiles genutzt wird.
Alle Rechner, welche aus dem Internet erreichbar sind, können dadurch angreifbar sind.
Link zur Quelle.
Log4j wird in den meisten Produkten von Teamcenter und Schnittstellen auf Servern und Clients benutzt.

Betroffen sind alle Versionen von «log4j-core» ab Version 2.
Ab 2.16.0 oder neuer sind die Jars nicht mehr betroffen.
Bitte leiten Sie dies an Ihren Systemadministrator zur umgehenden Überprüfung/Umsetzung weiter:

1.1 Analyse

- Auf Server und Clients nach dieser Datei suchen (Suche auf C:, D:, etc.). Es sind laut BSI nur Dateien ab Version 2.x betroffen:

  log4j-core-2.*.jar

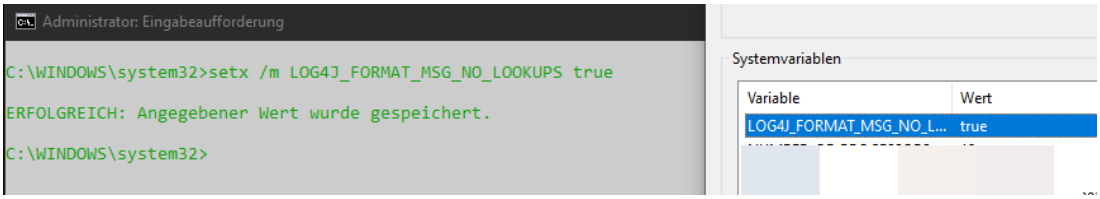


  Alternativ kann auch ein Freeware Tool dafür benutzt werden:
  https://github.com/mergebase/log4j-detector
  Log4j Versionen 2.16.0 oder neuer sind nicht verwundbar.

1.2 Systemvariable

- Das Setzen der Systemvariable war Abhilfe für Versionen zwischen 2.10 und 2.15.
  Dies scheint nach neuen Erkenntnissen nicht mehr auszureichen.
  Setzen Sie diese Variable auf Servern und Clients!
  LOG4J_FORMAT_MSG_NO_LOOKUPS = true

  bzw. CMD als Admin:
  setx /m LOG4J_FORMAT_MSG_NO_LOOKUPS true



1.3 Klasse in JARs löschen

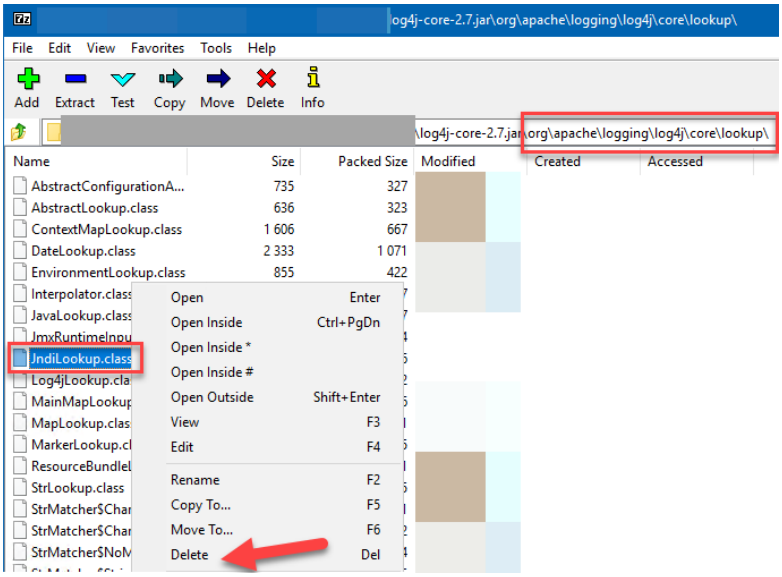
- Bei allen Versionen kleiner 2.16* dann muss in jeder dieser JAR Files die betroffene Kasse gelöscht werden. Achten Sie darauf, dass kein Service auf dem File läuft, sonst lässt sich das File nicht bearbeiten. (*aktueller Stand 17.12.21)

- Das JAR-File kann mit 7zip geöffnet und die betroffene Klasse von Hand gelöscht werden.

  (rechte Maus auf das JAR – 7zip – open archive), dann in der Struktur dieses File Löschen:
  org/apache/logging/log4j/core/lookup/JndiLookup.class
  (Die betroffene Klasse ist wird nicht für die normale Funktion von Teamcenter benötigt.)

- Variante als Script:

```
cd /d [7-zip Install Verzeichnis]
@rem verify the JndiLookup.class file exists in the .jar file
7z l log4j-core-2.07.0.jar | findstr /i /c:JndiLookup
@rem remove the JndiLookup.class file
7z d log4j-core-2.07.0.jar   JndiLookup.class  -r
@rem verify the JndiLookup.class file no longer exists in the .jar file
7z l log4j-core-2.07.0.jar | findstr /i /c:JndiLookup
```



1.4 NEUSTART

- Nach all den Aktionen müssen alle Dienste neugestartet werden. Ein Server/Client Neustart bietet sich an.

2 Log4j (ENGLISH v.1.2 – 17.12.21)

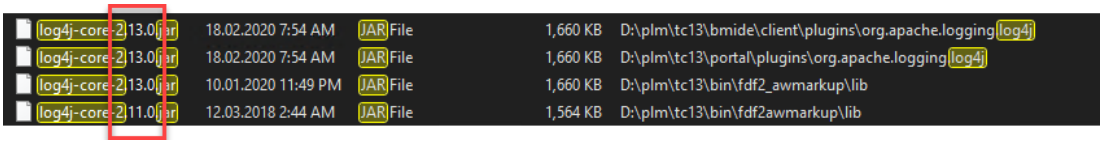
There is a critical vulnerability in the open source module **log4j**, which is used by Java for log files.
All computers that are accessible from the Internet can be attacked by this.
Link to source.
Log4j is used in most Teamcenter products and interfaces on servers and clients.

All versions of "**log4j-core**" from version 2 are affected.
2.16.0 or newer are no longer affected.
Please forward this to your system administrator for immediate review/implementation:

2.1 Analysis

- Search for this file on server and clients (search on C:, D:, etc.).
  According to BSI, only files from version 2.x are affected:

  log4j-core-2.*.jar

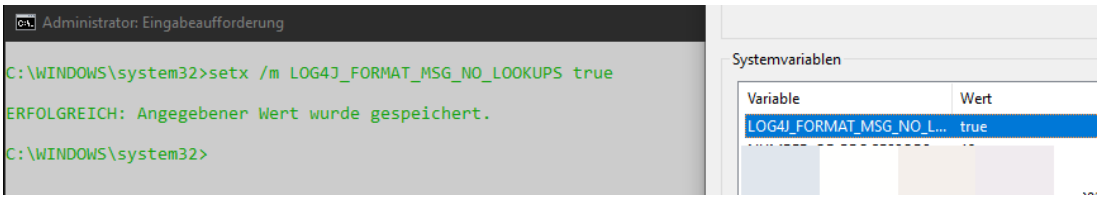


  Alternatively, a freeware tool can be used for this purpose:
  https://github.com/mergebase/log4j-detector
  Log4j versions 2.16.0 or later are not vulnerable.

2.2 System Variable

- Setting the system variable was workaround for versions between 2.10 and 2.15.
  According to new findings, this no longer seems to be sufficient.
  Set this variable on servers and clients!
  LOG4J_FORMAT_MSG_NO_LOOKUPS = true

  or use CMD as admin:
  setx /m LOG4J_FORMAT_MSG_NO_LOOKUPS true



2.3 Delete class in JARs

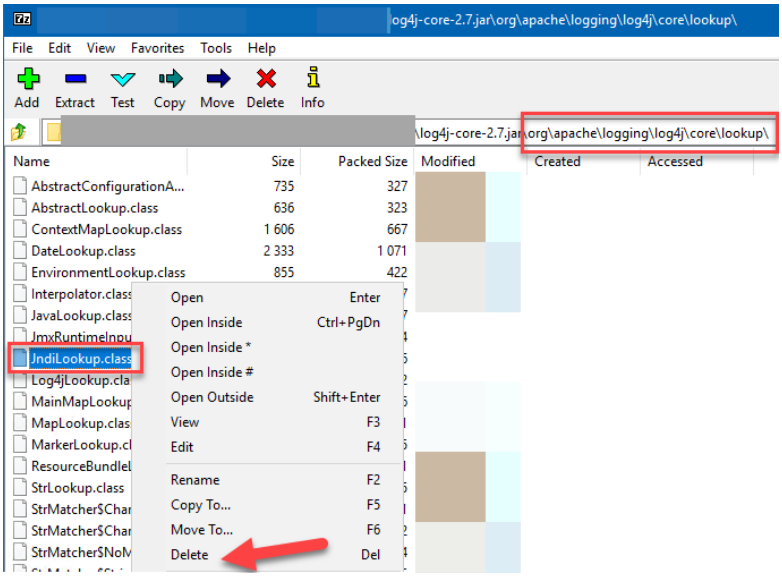
- For all versions smaller than 2.16* the class affected class must be deleted in each of these JAR files. Make sure that no service is running on the file, otherwise the file cannot be edited.
  (*aktueller Stand 17.12.21)

- The affected JAR file can be opened with 7zip and the affected class deleted by hand.

  (right mouse click on the JAR - 7zip - open archive), then in the structure delete this file:
  org/apache/logging/log4j/core/lookup/JndiLookup.class
  (The affected class is not needed for the normal function of Teamcenter).

  Variant as script:

```
cd /d [7-zip Install Verzeichnis]
@rem verify the JndiLookup.class file exists in the .jar file
7z l log4j-core-2.07.0.jar | findstr /i /c:JndiLookup
@rem remove the JndiLookup.class file
7z d log4j-core-2.07.0.jar   JndiLookup.class  -r
@rem verify the JndiLookup.class file no longer exists in the .jar file
7z l log4j-core-2.07.0.jar | findstr /i /c:JndiLookup
```



2.4 RESTART

- After all the action, all services must be restarted. A server/client restart is a good idea.