Gestalten Sie Ihre Dokumentenprozesse von morgen

Empfohlene Sofortmaßnahmen für PROXESS-Produkte (Update 21-12-16)

zur BSI-Sicherheitswarnung für log4j

Aufgrund aktueller Entwicklung und Meldungen von Sicherheitsunternehmen reagieren wir mit diesem Dokument auf die veränderte Lage. Dieses Dokument ersetzt unser Schreiben vom 14.12.2021. Die empfohlene Methode zur Absicherung Ihres Systems durch Setzen einer Umgebungsvariablen ist nicht ausreichend. Ein Update der log4j Dateien auf die Version 2.16 ist unumgänglich.

Wir, die PROXESS GmbH sowie unsere Vorlieferanten, arbeiten zusätzlich daran, unsere zukünftigen Installations- und Setupsätze mit den gesicherten log4j Dateien auszustatten.

Diese Handlungsempfehlungen erfolgen nach besten Wissen und Gewissen. Es ist nicht auszuschließen, dass in der Folge noch weitere Maßnahmen notwendig werden. Wir versuchen Sie immer schnellstmöglich auf dem Stand der Dinge zu halten.

Weiterführende Fragen beantworten wir unter der Mailadresse:

CVE202144228@proxess.de

Dieses Dokument beschreibt das Vorgehen, um folgende Produkte der PROXESS GmbH gegen die Sicherheitslücke CVE-2021-44228 von log4j abzusichern.

(siehe: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.html)

Relevante Produkte und Softwarelösungen:

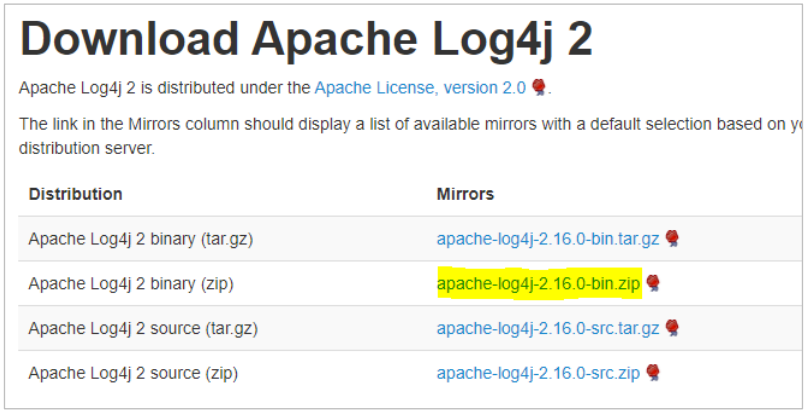
1. PROXESS Belegleser (PROXESS Xtract, smartFix)
2. PROXESS Workflow (PROXESS Documents, PROXESS Contract, PROXESS Personal)
3. PROXESS DMS (PROXESS professional)
4. PROXESS Web Client (Viewing Komponente, PrizmDoc)
5. HABEL Belegleser, HABEL Postkorb, HABEL ARCHIV

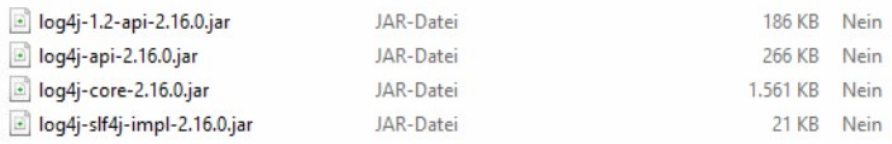
1. Vorbereitung

1. **ERSTELLEN SIE EIN BACKUP IHRER SYSTEME** (Dies sollte selbstverständlich sein, aber einmal mehr daran zu erinnern, schadet nicht. 😊)

2. Laden Sie die aktuelle Version von Log4j (Version >= 2.16) von folgender URL

   https://logging.apache.org/log4j/2.x/download.html





   Achten Sie darauf, dass die Versionsnummer >= 2.16 verwendet ist.

4. Folgen Sie den Handlungsempfehlung für die von Ihnen eingesetzten Produkte.

2. PROXESS Belegleser

Die Analyse unseres Vorlieferanten Insiders Technologies GmbH, Kaiserslautern hat ergeben, dass die von uns verwendeten und eingesetzten Produkte der smartFix-Produktfamilie nicht von der log4j Sicherheitslücke betroffen sind.

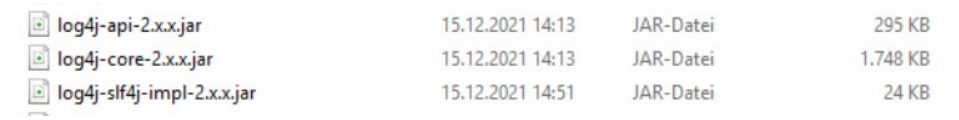
3. PROXESS Workflow

Betroffene Produktversion ab: DOCUMENTS-Installationen ab DOCUMENTS 5.0f - 2205

Empfohlene Sofortmaßnahme: Ersetzen Sie die verwendeten log4j-Dateien

1. Navigieren Sie in das Verzeichnis
   [INSTALLDIR]\tomcat8\webapps\documents\WEB-INF\lib

   INSTALLDIR z.B. C:\Program Files\Documents5

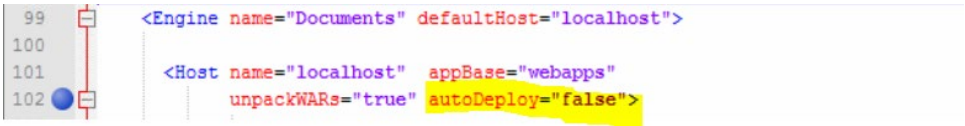


3. Kopieren Sie die in 1. Vorbereitung extrahierten Dateien in das Verzeichnis
   [INSTALLDIR]\tomcat8\webapps\documents\WEB-INF\lib

4. Bennen Sie Dateien um. Ersetzen Sie die Versionsnummer 2.16.0 durch 2.x.x

5. Navigieren Sie in das Verzeichnis
   [INSTALLDIR]\tomcat8\conf

6. Editieren Sie die Datei server.xml und setzen Sie in Zeile 102 den Parameter
   autoDeploy="false" (siehe Screenshort)



7. Starten Sie entweder den Tomcat Web Server Dienst oder alternativ den gesamten
   Server neu.

Hinweis:
Löschen Sie in keinem Fall das Verzeichnis [INSTALLDIR]\tomcat8\ webapps\documents
Dies führt zum Verlust Ihrer kundenindividuellen Konfiguration und installiert die vulnerablen log4j-Dateien erneut.

4. PROXESS DMS

Betroffene Produktversion: ab PROXESS 10 2020R2 (Dateiversion 12.x)

Empfohlene Sofortmaßnahme: Ersetzen Sie die verwendeten log4j Dateien

1. Öffnen Sie einen Command Prompt (cmd)

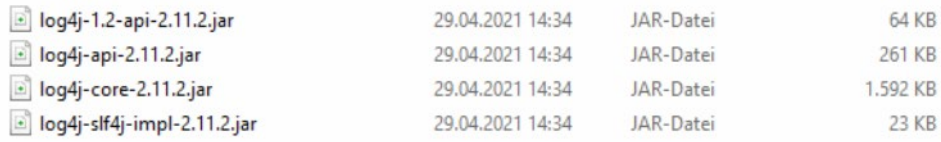
2. Navigieren Sie in das Verzeichnis
   [INSTALLDIR]\PROXESS Solr\bin

   INSTALLDIR z.B. C:\Program Files (x86)\PROXESS

3. Führen Sie das folgende Kommando aus: solr.cmd stop –p 8075

4. Navigieren Sie in das Verzeichnis
   [INSTALLDIR]\PROXESS Solr\server\lib\ext

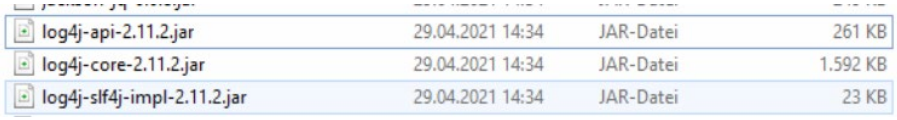
5. Verschieben Sie die folgenden Dateien in ein temporäres Verzeichnis z.B. c:\temp



6. Kopieren Sie die in 1. Vorbereitung extrahierten Dateien in das Verzeichnis
   [INSTALLDIR]\PROXESS Solr\server\lib\ext

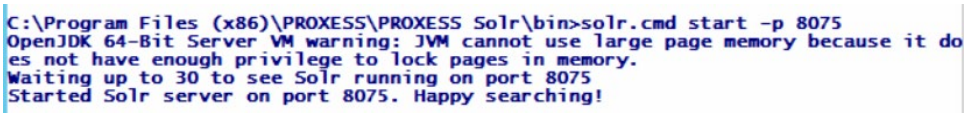
7. Navigieren Sie in das Verzeichnis
   [INSTALLDIR]\PROXESS Solr\contrib\prometheus-exporter\lib

8. Löschen Sie die Dateien



9. Kopieren Sie die in 1. Vorbereitung extrahierten Dateien in das Verzeichnis
   [INSTALLDIR]\PROXESS Solr\contrib\prometheus-exporter\lib

10. Führen Sie das folgende Kommando aus: solr.cmd start –p 8075
    Nachfolgender Screenshot beschreibt einen erfolgreichen Neustart



PROXESS DMS Systeme, die die Volltextdatenbank Lucene (vor PROXESS 10 2020R2) verwenden, nutzen auch log4j. Diese werden jedoch so eingesetzt, dass sie nicht in einer schädlichen Art und Weise ausgenutzt oder angegriffen werden können. (Es wird kein erreichbarer HTTP-Server verwendet.)

5. PROXESS Web Client

Betroffene Produktversion: alle Produktversionen, die den PROXESS Web Client (PROXESS Scribe, PrizmDoc Datei Renderering Service) verwenden.

Empfohlene Sofortmaßnahme: Austausch der log4j-Dateien gegen die aktuell vom BSI empfohlenen Dateiversionen

1. Lokalisieren Sie für den Prizm Rendering Service die älteren Dateiversionen
   Windows System: [INSTALLDIR]:\libs\javaservices
   INSTALLDIR z.B. c:\PRIZM
   Linux System: ./usr/share/prizm/libs/javaservices

2. Sichern Sie die vorhandenen log4j-Dateien in einem separaten Verzeichnis (z.B. c:\temp) und löschen Sie diese danach im oben genannten Ursprungsverzeichnis. Auf Windows Systemen muss eventuell der Prizm Service vorher gestoppt werden.

3. Kopieren Sie die in 1. Vorbereitung extrahierten Dateien in das Verzeichnis
   Windows System: [INSTALLDIR]:\libs\javaservices
   Linux System: ./usr/share/prizm/libs/javaservices

4. Starten Sie den Prizm Service neu.
   Windows System: Verwenden Sie services.msc (Windows Dienste).
   Linux System: Führen Sie auf der Console den Befehl: ‘reboot now’ aus.

5. Prüfen Sie den erfolgreichen Neustart (kann mehrere Minuten dauern) indem Sie in Ihrem Browser folgende Adresse eingeben

   http://[SERVER]:18681/admin

   Server z. B. Name des Prizm Servers oder IP-Adresse des Prizm Servers

6. HABEL Archiv

In den HABEL Produktversionen 2015 (abgekündigt zum 31.12.2021), 2016, 2017 und R21 gehören die log4j-Dateien nicht zum Standardinstallationsumfang. Produktversionen kleiner 2015 sind bereits seit längerem abgekündigt, so dass hierfür in dieser Information keine Aussage getroffen wird.

Für den Betrieb Ihrer HABEL Software sind weitere Softwarekomponenten von Drittanbietern notwendig (z.B. Apache Webserver). Hier können vulnerable log4j Dateien installiert worden sein. Prüfen Sie dies gemäß ‘7- Sonstiges’

7. Sonstiges

Unabhängig zur den genannten Ad-Hoc Maßnahmen, können Sie zur generellen Überprüfung Ihrer Systeme auf das Vorhandensein von log4j folgendes Powershell-Skript verwenden. Öffnen Sie dazu die Windows Powershell mit administrativen Rechten und führen auf jedem Festplattenlaufwerk diesen Befehl aus:

```
gci 'C:\' -rec -force -include *.jar -ea 0 | foreach {select-string "JndiLookup.class" $_} | select -exp Path
```

Als Ergebnis erhalten Sie alle Fundstellen der Datei log4j-core-x.xx.x.jar (x.xx.x steht für die installierte Dateiversion). Sollten hierbei log4j Versionen <= 2.15.0 aufgelistet sein, handeln Sie gemäß der Empfehlung der betroffenen Produktlieferanten.

Hinweis: Dieses Skript findet gegebenenfalls auch die log4j-Dateien, die Sie in den vorherigen Schritten in das Verzeichnis c:\temp verschoben habe. Diese können Sie ignorieren.

Sollten die Fundstellen auf die Produkte HABEL oder Lucene hinweisen so setzen Sie sich bitte mit dem Kundensupport (https://customer.proxess.de/supportticket-erstellen) in Verbindung