Problemstellung[1]:

Log4j ist eine beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung. Das Blog eines Dienstleisters für IT-Sicherheit [LUN2021] berichtet über die Schwachstelle CVE-2021-44228 [MIT2021] in log4j in den Versionen 2.0 bis 2.14.1, die es Angreifern gegebenenfalls ermöglicht, auf dem Zielsystem eigenen Programmcode auszuführen und so den Server zu kompromittieren. Diese Gefahr besteht, wenn log4j verwendet wird, um eine vom Angreifer kontrollierte Zeichenkette wie beispielsweise den HTTP User-Agent zu protokollieren.

Aufgrund der weiten Verbreitung der Bibliothek ist es nur schwer absehbar, welche Produkte betroffen sind.

Maßnahme:

Der Hersteller empfiehlt als Maßnahme, die auch in log4J Versionen ab 2.0-beta9 und höher funktioniert, die Klasse `JndiLookup` aus dem Klassenpfad zu löschen [APA2021b].

Die Klasse `JndiLookup` findet in Doxis4 keine Verwendung und kann entfernt werden. Aktuell gibt es eine Reihe vom BSI veröffentlichen Tools, die hierbei unterstützen. SER empfiehlt (automatisiert) folgende Vorgehensweise zur Mitigation (Schließen der Sicherheitslücke):

1. Stoppen der Anwendung
2. Suchen aller betroffenen Container (auch innerhalb von WAR-Containern etc.)
3. Backup der betroffenen Container
4. Entfernen der Klasse `JndiLookup` [2]
5. Neustart der Anwendung

Das BSI und National Cyber Security Centrum NCSC referenziert hier auf folgende Tools zur Unterstützung bei der Durchführung der oben angegebenen Maßnahmen:

- https://github.com/NCSC-NL/log4shell
- https://github.com/NCSC-NL/log4shell/blob/main/scanning/README.md
- https://github.com/logpresso/CVE-2021-44228-Scanner

SER empfiehlt die Nutzung des folgenden Tools:

- https://github.com/logpresso/CVE-2021-44228-Scanner

unter Berücksichtigung der folgenden Hinweise:

a) Das Tool sollte nur von Administratoren ausgeführt werden, die über einen entsprechenden technischen Hintergrund verfügen.

b) Das Tool darf ausschließlich auf die Standard-Doxis4-Installationsverzeichnisse angewendet werden.

c) Diese Maßnahme ist zunächst auf den Entwicklungssystemen und Testsystemen auszuführen.

d) Im Anschluss sind abschließende Regressionstests durchzuführen.

---

[1] *Hinweis: Es handelt sich bei diesem Dokument um einen technischen Leitfaden, dessen Inhalt auch aus fremden Quellen zusammengetragen wurden.*
Quelle BSI: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=8

[2] *Das Löschen der JNDI Lookup Klasse wird nach neusten Erkenntnissen des NIST als der bessere Weg erachtet. Quelle NIST CVE-2021-45046:* https://nvd.nist.gov/vuln/detail/CVE-2021-45046

e) Erst nach erfolgreichen Tests darf eine Anwendung in Produktivsystemen erfolgen.

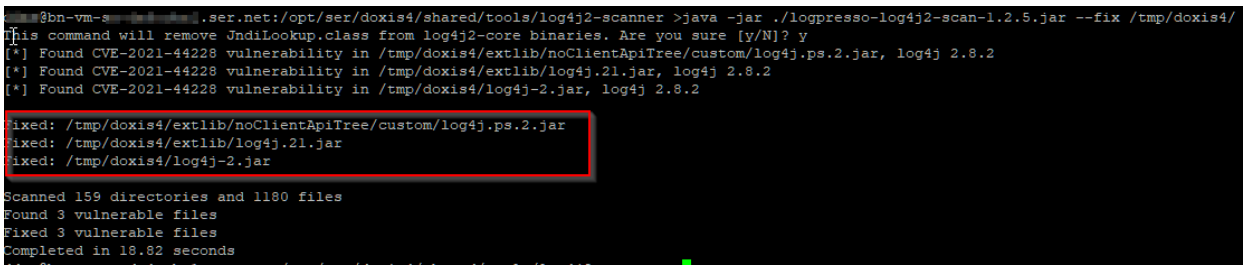
f) Etwaige interne Regelungen zur IT-Sicherheit sind jeweils zu beachten. Insbesondere sind gegebenenfalls die zuständigen internen Stellen wie beispielsweise der IT-Sicherheitsbeauftragte mit einzubeziehen.

Das Tool führt automatisiert unter Angabe eines Pfades die oben genannten Schritte 2-4 durch. Es ergibt sich insgesamt folgende Abfolge:

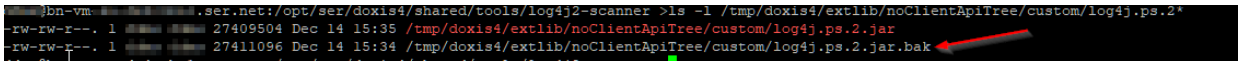
i. Stoppen der Doxis4-Anwendungen

ii. Ausführen des folgendes Befehls unter Angabe des Doxis4-Installationsverzeichnisses:
`java -jar logpresso-log4j2-scan.jar --fix --trace target_path_doxis4_installation`

iii. Neben den korrigierten Versionen befindet sich im selbigen Verzeichnis eine `*.bak` Datei, also eine Backup Datei zum jeweiligen Container im Ursprungsformat. In der Ausgabe des Kommandos sind die korrigierten Versionen unter der Sektion “fixed” aufgelistet.



Beispiel einer `bak`-Datei:



Hinweis: Da die `bak`-Dateien auch vom Classloader geladen werden können, müssen diese aus den jeweiligen Verzeichnissen entfernt und gesichert werden (in ein Verzeichnis außerhalb eines Java- Classloadings). Der ursprüngliche Pfad der `bak`-Dateien muss mitgesichert werden.

iv. Starten der Doxis4-Anwendungen.

Wir empfehlen die Umsetzung der oben genannten Maßnahmen nach erfolgreichen internen Tests im Hause der SER. Wir weisen darauf hin, dass diese auf einer standardisierten Umgebung durchgeführt wurden und nicht alle Kundensysteme individuell abgebildet werden können.

Fallback-Szenario:

Kommt es bei den oben angegebenen Schritten zu Problemen, kann der ursprüngliche Zustand wiederhergestellt werden, indem der betroffene *`.bak` Container nach Stoppen der Doxis4-Anwendung zurückgesichert wird. Danach muss die Doxis4-Anwendung wieder gestartet werden.