Log4j-Sicherheitslücke

Karlsruhe // 12.2021 – Version 5

„log4j ist ein Framework zum Loggen von Anwendungsmeldungen in Java. Innerhalb vieler Open-Source- und kommerzieller Softwareprodukte hat es sich über die Jahre zu einem De-facto-Standard entwickelt. log4j gilt als Vorreiter für andere Logging-Frameworks, auch in anderen Programmiersprachen.“

log4j – Wikipedia

In dieser Bibliothek ist eine schwere Sicherheitslücke entdeckt worden.

„Die Sicherheitslücke kann dafür sorgen, dass Angreifer unter Umständen ihren Softwarecode auf den Servern ausführen können. Damit könnten sie zum Beispiel ihre Schadprogramme dort laufen lassen. Die Schwachstelle ist auf einige Versionen der Bibliothek mit dem Namen Log4j beschränkt. Allerdings hat niemand einen vollen Überblick darüber, wo überall die gefährdeten Versionen von Log4j genutzt werden.“

BSI: Warnstufe Rot: Software-Sicherheitslücke alarmiert Bundesamt - n-tv.de

STP
The Legal Tech Company

STP-Schnittstellen:

winsolvenz.p3 und winsolvenz.p4
Nicht betroffen, da kein Java verwendet wird.

Crystal Reports
Nicht betroffen, da kein log4j verwendet wird. Der Webserver nutzt log4javascript, aber dieses ist **nicht betroffen**.

GIS 1.0
Nicht betroffen, da kein Java verwendet wird.

GIS 4.0
Nicht betroffen, da kein Java verwendet wird.

Statistik Gateway
Nicht betroffen, da kein Java verwendet wird.

Vergütungsplaner & ForStaB
Nicht betroffen, da kein Java verwendet wird.

winsolvenz.BI
Nicht betroffen, da kein Java verwendet wird.

LEXolution.DMS
Nicht betroffen, da kein Java verwendet wird.

iDESK App
Nicht betroffen, da kein Java verwendet wird.

CompareDocs
STP liegen bisher keine Informationen des Herstellers vor. Der Hersteller Litera ist derzeit noch in der Analyse und hat bisher keine Aussage gegenüber STP getroffen.

LEXolution.KMS
Nicht betroffen, da kein Java verwendet wird.

LEXolution.BI
Nicht betroffen, da kein Java verwendet wird.

LEXolution.Contact
Nicht betroffen, da kein Java verwendet wird.

LEXolution.FoMa
Nicht betroffen. Verwendet nur log4javascript, was **nicht betroffen** ist.

LEXolution.Time
Nicht betroffen, da kein Java verwendet wird.

beA DESK

Im Hinblick auf beA DESK ist ein Angriffsszenario sehr unwahrscheinlich, da es keine Serverfunktionalität beinhaltet und deshalb nicht offen zugänglich ist.

Die bislang veröffentliche Anleitung zur Absicherung von bea DESK wird mit der Installation von bea DESK 1.2 Patch 2 obsolet. Die Umgebungsvariable wird nun vom bea DESK selber gesetzt. Weiterhin verwendet bea Connect die log4j Bibliothek in der Version 2.16. **Sollten Sie bereits die Umgebungsvariable gesetzt haben, müssen sie diese nun wieder entfernen. Dies gilt nur für den bea DESK 1.2 Patch 2 oder den Hotfix auf unserer Webseite herunterladen.**

Wenn sie noch einen bea DESK 1.2 Patch 1 oder älter verwenden, empfehlen wir Ihnen weiterhin dennoch, aktiv zu werden und folgende Schritte vorzunehmen. Die genaue Anleitung finden Sie hier.

Durch folgende verwendete Dritthersteller-Software besteht kein Sicherheitsrisiko:
- SecSigner (+ Software für Card-Reader) – laut Hersteller wird log4j im Produkt nicht eingesetzt.

Eureka-Winsolvenz

Nicht direkt betroffen, da kein Java verwendet wird.

Indirekt betroffen durch Dritthersteller-Software:
- Governikus Communicator Justiz Edition ist leider betroffen, allerdings gibt es bereits ein Update.
- Governikus Signer ist leider betroffen und es gibt leider kein Update.

Durch folgende verwendete Dritthersteller-Software besteht kein Sicherheitsrisiko:
- SecSigner (+ Software für Card-Reader) – laut Hersteller wird log4j im Produkt nicht eingesetzt.

WinJur

Nicht betroffen, da kein Java verwendet wird.

AutoStore

Benutzt Log4j over SLF4j v1.7.7
Die ControlSuite der Scansoftware Autostore von der Firma Kofax enthält die log4j Version 1.7.7. Der Hersteller hat uns daher mitgeteilt, dass Autostore und auch die ControlSuite nicht von der Sicherheitslücke betroffen sind.

Das BSI hat inzwischen folgende Information veröffentlicht:
"Entgegen der anderslautenden ursprünglichen Annahme ist Berichten zufolge die Programmbibliothek auch in den Versionen 1.x verwundbar. In diesen Fällen sei die Verwundbarkeit jedoch nur über eine schadhafte Programmkonfiguration ausnutzbar, sodass eine Ausnutzung weit weniger wahrscheinlich erscheint."

Wir warten aktuell auf die erneute Rückmeldung des Herstellers Kofax, ob die Beurteilung daher anders ausfällt.

Insolvenzportal

Nicht betroffen, da kein Java verwendet wird.

STP-Cloud

Nicht betroffen.
Das von uns verwendete ElasticSearch in der Version 7 ist laut Hersteller nicht von der Remote Code Execution betroffen. Von der Information Leakage war das von uns verwendete ElasticSearch in der Version 7 laut Hersteller ebenfalls nicht betroffen, da es nicht auf einer betroffenen Java-Version (JVM8 oder daruter, sondern auf JVM13) läuft.
Trotzdem haben wir die betroffene Einstellung in Java deaktiviert und damit eine zusätzliche Sicherheitsmaßnahme eingeleitet (ES_JAVA_OPTS: -Xms1g -Xmx1g -Dlog4j2.formatMsgNoLookups=true).

Von unserem Hostinganbieter Gridscale haben wir außerdem noch die Aussage erhalten, dass bereits am 11. & 12. Dezember alle internen Systeme auf die gemeldete Schwachstelle überprüft und die empfohlenen Maßnahmen umgesetzt wurden.