Änderungshistorie

Version	Datum	Autor	Stichworte
1.0	14.12.2021	Blomesystem GmbH	Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228), CSW-Nr. 2021-549032-1432, Version 1.4, 13.12.2021

Inhalt

1. Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat unter dem Titel "Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)" auf eine IT-Bedrohungslage der Stufe 4 / Rot hingewiesen. Im hier vorliegenden Schreiben wird auf das entsprechende Dokument des BSI (CSW-Nr. 2021-549032-1432, Version 1.4, 13.12.2021) Bezug genommen. Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen: TLP:WHITE: Unbegrenzte Weitergabe [https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=8].

Common Vulnerabilities and Exposures (CVE – deutsch Bekannte Schwachstellen und Anfälligkeiten) ist ein dem US-amerikanischen National Cybersecurity FFRDC unterstelltes und durch die Mitre Corporation gepflegtes Referenzier-System, dessen Ziel die Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen ist.
Am 26.11.2021 wurde unter der CVE-ID 'CVE-2021-44228' ein Eintrag mit folgender Beschreibung erfasst [https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228]:

original: Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. In previous releases (>2.10) this behavior can be mitigated by setting system property "log4j2.formatMsgNoLookups" to "true" or it can be mitigated in prior releases (<2.10) by removing the JndiLookup class from the classpath (example: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class).
deutsche Übersetzung (ohne Gewähr): Apache Log4j2 <=2.14.1 JNDI-Funktionen, die in Konfiguration, Protokollnachrichten und Parametern verwendet werden, schützen nicht vor angreifergesteuertem LDAP und anderen JNDI-bezogenen Endpunkten. Ein Angreifer, der Protokollnachrichten oder Protokollnachrichtenparameter kontrollieren kann, kann beliebigen Code ausführen, der von LDAP-Servern geladen wird, wenn die Ersetzung der Nachrichtensuche aktiviert ist. Ab log4j 2.15.0 ist dieses Verhalten standardmäßig deaktiviert. In früheren Versionen (> 2.10) kann dieses Verhalten durch Setzen der Systemeigenschaft "log4j2.formatMsgNoLookups" auf "true" oder in früheren Versionen (< 2.10) durch Entfernen der JndiLookup-Klasse aus dem Klassenpfad (Beispiel: zip - q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class) gemildert werden.

2. Hinweise zu Softwarekomponenten

2.1. Basissoftware blomesystem®

Die Basissoftware blomesystem® der Blomesystem GmbH inkl. der Web Feature Erweiterung basiert nicht auf JAVA-Technologie und ist daher von der kritischen Schwachstelle in log4j **nicht betroffen**.

2.2. Auf blomesystem® basierende LIMS-Applikationen, z.B. LABbase®

Die mit der Basissoftware blomesystem® erstellten LIMS-Applikationen basieren nicht auf JAVA-Technologie und sind daher von der kritischen Schwachstelle in log4j **nicht betroffen**.

2.3. Datenbanken

Die meisten Softwareprodukte der Blomesystem GmbH nutzen relationale Datenbanken zur Speicherung von Daten. Unsere Kunden setzen dabei Oracle- oder MS SQL Server-Datenbanken ein.
Beide Anbieter haben Informationen zum Thema bereitgestellt. Zum Zeitpunkt der Erstellung des vorliegenden Dokumentes waren diese unter den im Folgenden angegebenen Links verfügbar.

2.3.1. ORACLE-Datenbanken

Oracle hat Informationen wie folgt bereitgestellt:

> "Oracle Security Alert Advisory - CVE-2021-44228"
> [https://www.oracle.com/security-alerts/alert-cve-2021-44228.html]
>
> Gemäß Oracle - My Oracle Support ist unter dem Eintrag "Apache Log4j Security Alert CVE-2021-44228 Products and Versions (Doc ID 2827611.1)" ausgewiesen, dass "Oracle Database" und "Oracle Client" nicht betroffen sind.

2.3.2. MS SQL Server-Datenbanken

Microsoft hat Informationen wie folgt bereitgestellt:

> Microsoft Security Response Center
> "Microsoft's Response to CVE-2021-44228 Apache Log4j 2"
> [https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/]

2.4. blomesystem® LIMS-Applikationen und Schnittstellen zu Fremdsystemen

Bei vielen blomesystem® LIMS-Applikationen unserer Kunden werden die verschiedensten Schnittstellen als Datenempfänger oder -lieferanten angesprochen. Die zur LIMS-Applikation gehörenden Module und Optionen zur Anbindung der Fremdsysteme basieren nicht auf JAVA-Technologie und sind daher von der kritischen Schwachstelle in log4j **nicht betroffen.**

Darüber, inwieweit die Fremdsysteme, zu denen eine Schnittstelle etabliert wurde, von der aktuellen Problematik betroffen sind, können ausschließlich die Hersteller der Systeme weitergehende Auskunft erteilen.

2.5. Weitere Systeme und Add Ons der Blomesystem GmbH

2.5.1. ENMO®hydro / readyLIMS®

Die Softwareprodukte ENMO®hydro und readyLIMS® basieren nicht auf JAVA-Technologie und sind daher von der kritischen Schwachstelle in log4j **nicht betroffen**.

2.5.2. Probenahme-App

Die Probenahme-App der Blomesystem GmbH basiert nicht auf JAVA-Technologie und ist daher von der kritischen Schwachstelle in log4j **nicht betroffen**.

2.5.3. blomesystem® QDI

Die Schnittstelle zu SAP QM-IDI basiert nicht auf JAVA-Technologie und ist daher von der kritischen Schwachstelle in log4j **nicht betroffen**.

2.5.4. blomesystem® LabDDI

Das Schnittstellenmodul zur standardisierten Datenübernahme der Blomesystem GmbH basiert nicht auf JAVA-Technologie und ist daher von der kritischen Schwachstelle in log4j **nicht betroffen**.

2.6. Third Party Software

2.6.1. Softwarelösung zur Unterstützung der Probenahme vor Ort

Aktuell erstellt die Blomesystem GmbH in Zusammenarbeit mit der Takwa GmbH aus Erfurt eine Softwarelösung, die als weitere Variante der Unterstützung der Probenahme vor Ort angeboten werden wird.

Die Softwarelösung setzt bei den serverseitigen Komponenten eine separate, eingebettete PostgreSQL-Datenbank sowie einen Apache-Webserver ein.

Zur PostgreSQL-Datenbank wird zunächst verwiesen auf:

> The PostgreSQL Global Development Group
> "PostgreSQL JDBC and the log4j CVE"
> [https://www.postgresql.org/about/news/postgresql-jdbc-and-the-log4j-cve-2371/]

Die Takwa GmbH hat ergänzend folgende Informationen zur Verfügung gestellt:

Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)

Hinweise der Takwa GmbH

Das Softwareprodukt Takwa FormServer verwendet die betroffene Bibliothek log4j in der Version 2.x nicht und verteilt die Bibliothek nicht auf Kundensysteme.
Die Takwa GmbH setzt zum Teil die Bibliothek log4j Version 1.x ein. Diese ist grundsätzlich nicht betroffen, solange die Funktion "JMSAppender" nicht aktiviert ist. In der Takwa-Umgebung ist dieser Parameter nicht eingeschaltet.
Nach der aktuellen Kenntnislage ist selbst bei eingeschalteter Funktion nicht damit zu rechnen, dass dies ähnlich auszunutzen ist, wie in der Version 2.x.

Allgemeine Sicherheitsstruktur und Empfehlungen

Die Takwa Software läuft fast ausschließlich in geschützten Umgebungen. Wir empfehlen unseren Kunden grundsätzlich, dies beizubehalten. Damit ist die Funktionalität nicht im Internet zu erreichen. Sollten mobile Clients über eine DMZ zu erreichen sein, so empfehlen wir dringend, ein SSL-Frontend (z.B. Apache httpd) zu betreiben, welches mit Client-Authentifizierung arbeitet, damit eine Kommunikation aus dem öffentlichen Internet mit dem Takwa FormServer unterbunden wird. Alternativ kann der Betrieb einer VPN-Infrastruktur verwendet werden.

Takwa GmbH
Erfurt, 14.12.2021

Bei der gemeinsam erstellten Softwarelösung sind, wie empfohlen, der Betrieb des FormServers in einer DMZ und die Kommunikation zwischen Client und Server über https vorgesehen.