xSuite
It's simple. It's digital.

Außerordentliche Produktinformation

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

Dokumentversion 16.12.2021

Inhaltsverzeichnis

1. Außerordentliche Produktinformation – Dezember 2021

Die BSI hat am 12.12.2021 eine "Alarm Stufe Rot"-Meldung zur Software log4j für die Versionen 2.0 - 2.14.1 ausgerufen.

In einer Folgemeldung vom 14.12.2021 wurde auch die Version 1.x als gefährdet beurteilt. Wir haben die Produkte, die im Folgenden aufgeführt werden, auch in Hinblick auf diese Schwachstelle überprüft.

Nähere Informationen finden Sie hier.

Informationen zu den einzelnen Produkten finden Sie in den folgenden Abschnitten.

2. Produkte

2.1. xSuite Cube

-nicht betroffen-

2.2. xSuite Sphere

2.2.1. Prediction Server

Patch erfolgte am 13.12. vormittags.

2.3. xSuite Prism

2.3.1. xSuite Archive

Das xSuite Archive nutzt derzeit noch Elasticsearch 2.3. Hier wird eine log4j Version 1.x genutzt, welche nicht betroffen ist.

In der folgenden Version des xSuite Archive (Q1/2022) wird Elastic Search 7.x eingesetzt. Die eingesetzte Version wird ebenfalls nicht (mehr) betroffen sein.

Update

Wir haben die Bedrohungslange bezüglich der log4j Version 1.x unter Beachtung der Hinweise des BSI und der darin verlinkten Quellen überprüft.

Im Auslieferungszustand des xSuite Archive liegt keine schadhafte Programmkonfiguration vor. Eine schadhafte Programmkonfiguration kann nur durch eine Person, die physikalischen Zugriff auf den Applikationsserver hat, erfolgen. Zudem wäre ein Neustart des IIS-Webservers erforderlich.

2.3.1.1. Bei Nutzung von Apache DS (lokale Benutzerverwaltung)

Wir empfehlen ein Update von Apache DS oder alternativ eine Portierung der Apache DS LDAP-Benutzer in die xSuite Encore eigene Benutzerverwaltung.

Update

Apache DS ist nur Bestandteil des xSuite Core. Wenn Sie einen xSuite Encore im Einsatz haben (ab xSuite Archive Version 1.2.2), sind Sie nicht betroffen.

Im xSuite Core ist Apache DS in der Version 1.2 implementiert. Dieser nutzt eine log4j Version 1.x.

Wir haben die Bedrohungslange bezüglich der log4j Version 1.x unter Beachtung der Hinweise des BSI und der darin verlinkten Quellen überprüft.

Im Auslieferungszustand des xSuite Archive liegt keine schadhafte Programmkonfiguration vor. Eine schadhafte Programmkonfiguration kann nur durch eine Person, die physikalischen Zugriff

auf den Applikationsserver hat, erfolgen. Zudem wäre ein Neustart des IIS-Webservers erforderlich.

2.3.2. xSuite Archive Mail

Der folgende Text ist die offizielle Stellungnahme unseres Partners Techarrow, der für xSuite Archive Mail (Content Access) verantwortlich ist:

Am 9. Dezember wurde eine Sicherheitslücke in log4j entdeckt. Obwohl contentACCESS auf .NET basiert, verwendet es ElasticSearch als Suchmaschine. ElasticSearch ist JAVA-basiert und verwendet ebenfalls log4j für den Logging-Dienst. Da diese Schwachstelle noch sehr frisch ist, sind alle Produktteams dabei, genau zu untersuchen, welche Komponenten und Produkte betroffen sind. Nachfolgend versuchen wir, einige der Informationen zusammenzutragen, die contentACCESS betreffen.

Die Schwachstelle (CVE-2021-44228)

Die Apache log4j-Bibliothek ermöglicht es Entwicklern, verschiedene Daten innerhalb ihrer Anwendung zu protokollieren. Unter bestimmten Umständen stammen die zu protokollierenden Daten aus Benutzereingaben. Sollte diese Benutzereingabe Sonderzeichen enthalten und anschließend im Kontext von log4j protokolliert werden, wird schließlich die Java-Methode lookup aufgerufen, um die benutzerdefinierte Remote-Java-Klasse im LDAP-Server auszuführen. Dies wiederum führt zu RCE auf dem Opferserver, der die verwundbare log4j 2-Instanz verwendet.

Weitere Informationen: https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/.

Log4J

Die Entwicklerteams untersuchen die Sicherheitslücke noch und arbeiten an einer korrekten und endgültigen Lösung für dieses Problem. Bis jetzt wurde noch keine offizielle Version veröffentlicht, die dieses Problem vollständig behebt. Die letzte RC (2.15.0-rc2) befindet sich in der Testphase und sollte die Sicherheitslücke vollständig beheben.

ElasticSearch

Die ElasticSearch-Teams untersuchen auch, welche Versionen von ElasticSearch von dieser Sicherheitslücke betroffen sind. Basierend auf den aktuellen Erkenntnissen ist Elasticsearch aufgrund der Verwendung des Java Security Managers nicht anfällig für Remote Code Execution durch diese Schwachstelle, jedoch ist der betroffene Teil von log4j in der Codebasis vorhanden. Um die Möglichkeit der Remotecodeausführung durch diese Schwachstelle vollständig zu beseitigen, müssen die log4j-Bibliotheken mit den Bibliotheken aktualisiert werden, die den anfälligen Code nicht enthalten. Diese Lösung ist einer der Zwischenvorschläge des log4j-Teams (`zip -q -dlog4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`).

contentACCESS Patch

Der log4j-Patch ist im Download-Center verfügbar. Dieser Patch enthält nicht das verwundbare Modul in log4j. Die folgenden Schritte sind erforderlich, um den Patch anzuwenden:

1. Laden Sie den Patch vom Download Center herunter:
   https://download.tech-arrow.com/index.php?p=Custom&dl=elastic-log4j-patch%28CVE-2021-44228%29-without-JndiLookup.zip

Alternativ können Sie die benötigten Dateien in der xSuite Knowledge Base herunterladen.

Sie finden die Dateien im Anhang zu dem Artikel "Urgent Product Information: Critical vulnerability in log4j published (CVE-2021-44228)".

Stellen Sie sicher, dass die ZIP-Datei nicht vom Betriebssystem blockiert wird.

2. Entpacken Sie das Paket. Das Paket enthält die folgenden 3 log4j-Module:
   - `log4j-core-2.15.0.jar`
   - `log4j-1.2-api-2.15.0.jar`
   - `log4j-api-2.15.0.jar`
3. Stoppen Sie den Dienst `GATE.contentAccess.Search` und den Dienst `Elasticsearch 5.2.2 (Elasticsearch)`.
4. Verschieben Sie die folgenden Dateien aus dem Ordner `C:\ProgramFiles\TECH-ARROW\contentACCESS.Search\Elastic\lib\`:
   - `log4j-core-2.7.jar`
   - `log4j-api-2.7.jar`
   - `log4j-1.2-api-2.7.jar`
5. Kopieren Sie die folgenden Dateien aus dem Patch in den Ordner `C:\Program Files\TECH-ARROW\contentACCESS.Search\Elastic\lib\`:
   - `log4j-core-2.15.0.jar`
   - `log4j-1.2-api-2.15.0.jar`
   - `log4j-api-2.15.0.jar`
6. Starten Sie den Dienst `Elasticsearch 5.2.2 (Elasticsearch)` und den Dienst `GATE.contentAccess.Search`.

2.3.3. xSuite 365 (Mailroom)

xSuite 365 (Mailroom) ist eine Anwendung, die im xSuite Core enthalten ist. Diese Anwendung setzt kein log4j ein und ist daher nicht betroffen.

2.3.4. xSuite Interface Prism

-nicht betroffen-

2.3.5. xSuite Capture Bus

-nicht betroffen-

2.3.6. xSuite Invoice Prism (Basis Otris Documents)

Im Verzeichnis `{Installationsverzeichnis}\Otris Documents\xSuiteRessources\wmd_%pem%\` existiert ein Verzeichnis `CatalogueImport`. Innerhalb dieses Verzeichnisses ist log4j im Code zu finden.

Dieses Verzeichnis ist jedoch Bestandteil eines anderen, abgekündigten Templates (Procurement) und wird nicht mehr genutzt.

Bei Bedarf kann folgendes getan werden:

1. Den genannten Ordner löschen
2. Den Windows-Service `DocumentsTomcat8` beenden
3. Das Verzeichnis `{Installationsverzeichnis}\Otris Documents\Tomcat8\WebApps\Documents` löschen
4. Das Verzeichnis `{Installationsverzeichnis}\Otris Documents\Tomcat8\Work\Documents` löschen
5. Den Windows-Service `DocumentsTomcat8` starten

2.3.7. xSuite Interface eInvoice

xSuite Interface eInvoice basiert auf dem xSuite Interface, welches nicht betroffen ist.

eInvoice setzt zur Validierung und Visualisierung externe Tools der KoSIT ein, zu welchen uns derzeit keine Informationen auf eine log4j-Schwachstelle vorliegen.

- KoSIT Validator (Koordinierungsstelle für IT-Standards · GitHub)
  - Keine Code-Referenzen auf log4j entdeckt
- KoSIT Visualization (Koordinierungsstelle für IT-Standards · GitHub)
  - Keine Code-Referenzen auf log4j entdeckt

2.4. Helix

-nicht betroffen-

2.5. Otris Documents

Innerhalb von Otris DOCUMENTS wird log4j in den Versionen DOCUMENTS 5g und 5f genutzt. Ältere Versionen sind nicht betroffen.

Otris hat einen Hotfix je Version bereitgestellt. Wenn Sie den zuvor gemeldeten Hotifx bereits umgesetzt haben, besteht kein Handlungsbedarf. Ansonsten empfehlen wir das Einspielen der offiziell ausgelieferten Hotfixes.

ACHTUNG
Bei inkorrekter Durchführung des Hotfix kann es passieren, dass beim Neustart des Services `DocumentsTomcat8` die folgende Datei verloren geht:

```
...\Documents5\tomcat8\conf\Documents\localhost\docu-
ments.xml
```

Sichern Sie diese Datei bevor Sie den Hotfix einspielen. Diese Datei wird für xSuite Invoice Prism benötigt.

Die Handlungsanweisungen, bereitgestellt durch Otris, finden Sie in der xSuite Knowledge Base in dem Artikel "Update 1 Urgent Product Information: Critical vulnerability in log4j published (CVE-2021-44228)".

2.6. Produkte der Easy Software AG

Die Easy Software AG prüft ihre Produkte in Verbindung mit log4j.

Folgende Produkte sind seitens Easy Software als nicht betroffen gemeldet:

- EASY Archive 6 & 7
- EASY for Exchange
- EASY for Dynamics NAV
- EASY for Dynamics 365 BC
- EASY for Dynamics 365 FO
- EASY for SAP
- EASY for SharePoint
- EASY for Notes
- EASY Capture Plus
- EASY X-Invoicing Services
- IRIS

Lediglich Easy DOCUMENTS und Easy ApiOmat sind als betroffen gemeldet. Zu allen anderen Software-Produkten, wie z. B.

- EASY xBASE
- EASY XML Server
- Easy Interface (EBIS)
- EASY-Archive kleiner Version 6 (z. B. EASY Enterprise x Easy i)
- etc.

liegen uns keine weiteren, Informationen seitens des Softwarehersteller Easy Software AG vor.

Aktuelle Informationen zu den Easy-Produkten finden Sie hier direkt bei der Easy Software AG.

2.7. Saperion

Wenn Sie ein Produkt von Hyland im Einsatz haben, z. B. Saperion, empfehlen wir den Abgleich Ihrer Produkte mit der offiziellen Verlautbarung von Hyland.

Diese finden Sie in der xSuite Knowledge Base in dem Artikel "Update 1 Urgent Product Information: Critical vulnerability in log4j published (CVE-2021-44228)".

3. Hinweis

Die Aussagen beruhen auf Analysen basierend auf den uns derzeit vorliegenden Informationen der BSI und den in der offiziellen Verlautbarung angegebenen Quellen.

Wir beobachten die Entwicklungen zu diesem Thema weiter. Sollten weitere Schwachstellen erkannt werden, werden diese kommuniziert und mit höchster Priorität in die Entwicklung gebracht.