3131789 - Schwachstelle für Log4j CVE-2021-44228 in SAP Business One mindern

Komponente: SBO-CRO-SEC (Sicherheit in SAP-Business-One-Software), Version: 7, Freigegeben am: 13.01.2022

Symptom

- Schwachstelle CVE-2021-44228 für log4j
- Auswirkungen auf SAP Business One
- log4j ist eine Apache-Bibliothek, die häufig in Java-Anwendungen verwendet wird. Dieses spezielle Problem wurde in **log4j2** festgestellt und in log4j 2.15.0 behoben.

Umgebung

SAP Business One

Auflösung

SAP stellt gemäß dem SAP-Hinweis 3131740 (https://launchpad.support.sap.com/#/notes/3131740) ein Feature Package bereit, das dieses Problem behebt. Kunden müssen SAP Business One FP2111 implementieren oder ein Upgrade darauf durchführen.

Behelfslösung

Bewerten Sie vor der Implementierung die Behelfslösung für Ihre SAP-Landschaft.

Beachten Sie, dass es sich bei dieser Behelfslösung um eine temporäre Korrektur und nicht um eine dauerhafte Lösung handelt. SAP empfiehlt dringend, die im Sicherheitshinweis beschriebenen Korrekturen einzuspielen, die anstelle der Behelfslösung oder nach dem Einspielen der Behelfslösung vorgenommen werden können.

Wenn Sie SAP Business One oder SAP Business One, Version für SAP HANA (Version >= 9.3 PL07 und <= 10.0 FP2108) verwenden und die Komponente Workflow installiert ist, können Sie die Schwachstelle für den Workflow mit der folgenden Vorgehensweise mindern:

1. Öffnen Sie das Paket *C:\Program Files (x86)\sap\SAP Business One ServerTools\Workflow\workflow-service.war* in winrar. (Klicken Sie mit der rechten Maustaste in winrar auf "Öffnen".)
2. Navigieren Sie zu *\WEB-INF\lib\log4j-core-2.13.3.jar*, und entfernen Sie die *Klasse JndiLookup* aus der Klasse classpath:*org/apache/logging/log4j/core/lookup/JnLookdiup.class.* Navigieren Sie für Version >= 9.3 PL07 und < 10.0 FP2008 zu \WEB-INF\lib\log4j-core-2.11.1.jar, und führen Sie den Vorgang aus.
3. Akzeptieren Sie das Aktualisierungsarchiv.
4. Starten Sie die *SAP Business One Workflow Engine* über die Windows-Dienste neu.

Wenn Sie SAP Business One (Version >= 10.0 FP 2008 und <= 10.0 FP 2108) verwenden und die Komponente Lizenzserver installiert ist, können Sie die Schwachstelle für den Lizenzserver mit der folgenden Vorgehensweise mindern:

1. Öffnen Sie das Paket *C:\Program Files (x86)\SAP\SAP Business One ServerTools\LicenseHTTPS\webapps\LicenseControlCenter.war* in winrar. (Klicken Sie mit der rechten Maustaste auf *LicenseControlCenter.war*, und öffnen Sie es mit winrar.)
2. Navigieren Sie zu *\WEB-INF\lib\log4j-core-2.7.jar*, und entfernen Sie die *Klasse JndiLookup* aus der Klasse classpath:*org/apache/logging/log4j/core/lookup/JndiLookup.class*.
3. Akzeptieren Sie das Aktualisierungsarchiv.
4. Starten Sie den *SAP Business One Server Tools Service* über die Windows-Dienste neu.

Wenn Sie SAP Business One (Version >= 10.0 FP 2008 und <= 10.0 FP 2108) verwenden und die Komponente Serviceschicht installiert ist, können Sie die Schwachstelle für die Serviceschicht wie folgt mindern:

1. Wechseln Sie zum Installationsordner der 64-Bit-Servertools (z.B. *C:\Programme\SAP\SAP Business One ServerTools*).
2. Navigieren Sie zum *Webapp-Ordner ServiceLayerController*:.*ServiceLayer\ServiceLayerController\webapps*
3. Klicken Sie mit der rechten Maustaste auf *ServiceLayerController.war*, und öffnen Sie es mit winrar.
4. Navigieren Sie zu *WEB-INF\lib\log4j-core-2.7.jar*, doppelklicken Sie darauf, um die Ordnerstruktur von *log4j-core-2.7.jar* anzuzeigen.
5. Suchen Sie die Datei *JndiLookup.class* im Klassenpfad: *org/apache/logging/log4j/core/lookup*, und löschen Sie diese Datei.
6. Akzeptieren Sie das aktualisierte Archiv.
7. Starten Sie den *64-Bit-Dienst für SAP-Business-One-Servertools* über die Windows-Dienste neu.

Wenn Sie SAP Business One (Version >= 10.0 FP 2105 und <= 10.0 FP2108) verwenden und die Komponente Job Service installiert ist, können Sie die Schwachstelle für den Job Service wie folgt mindern:

1. Öffnen Sie das Paket *C:\Program Files (x86)\SAP\SAP Business One ServerTools\ReportingService\webapps\ReportingService.war* in winrar. (Klicken Sie mit der rechten Maustaste in winrar auf "Öffnen".)
2. Navigieren Sie zu *\WEB-INF\lib\log4j-core-2.14.0.jar*, und entfernen Sie die *Klasse JndiLookup* aus der Klasse classpath:*org/apache/logging/log4j/core/lookup/JnLookdiup.class*.
3. Akzeptieren Sie das Aktualisierungsarchiv.
4. Starten Sie den *SAP Business One Server Tools Service* über die Windows-Dienste neu.

Wenn Sie SAP Business One (Version >= 10.0 FP 2008 und <= 10.0 FP 2108) verwenden und die Komponente Extension Manager (SLD) installiert ist, können Sie die Schwachstelle für Extension Manager wie folgt mindern:

1. Öffnen Sie das Paket *C:\Program Files (x86)\SAP\SAP Business One ServerTools\ExtensionManager\webapps\ExtensionManager.war* in winrar. (Klicken Sie mit der rechten Maustaste auf *ExtensionManager.war*, und öffnen Sie es in winrar.)
2. Navigieren Sie zu *\WEB-INF\lib\log4j-core-2.7.jar*, und entfernen Sie die *Klasse JndiLookup* aus der Klasse classpath:*org/apache/logging/log4j/core/lookup/JndiLookup.class.*
3. Akzeptieren Sie das Aktualisierungsarchiv.
4. Starten Sie den *SAP Business One Server Tools Service* über die Windows-Dienste neu.

Wenn Sie SAP Business One, Version für SAP HANA (Version >= 10.0 FP 2008 und <= 10.0 FP 2108) verwenden und die Komponente Lizenzserver installiert ist, können Sie die Schwachstelle für den Lizenzserver mit der folgenden Vorgehensweise mindern:

1. Wechseln Sie in das Installationsverzeichnis der Servertools (z.B. */usr/sap/SAPBusinessOne*).
2. Navigieren Sie zum Verzeichnis webapps der Lizenz:

/usr/sap/SAPBusinessOne/ServerTools/License/webapps

3. Führen Sie den folgenden Befehl aus, um die *JndiLookup.class* von log4j-core-2.7.jar aus *LicenseControlCenter.war* zu entfernen:

```
unzip LicenseControlCenter.war WEB-INF/lib/log4j-core-2.7.jar -d.
zip -q -d WEB-INF/lib/log4j-core-2.7.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
zip LicenseControlCenter.war WEB-INF/lib/log4j-core-2.7.jar
rm -r WEB-INF
```

4. Stellen Sie die Berechtigung von *LicenseControlCenter.war* wieder her, indem Sie den folgenden Befehl ausführen:

```
chown b1service0:b1service0 LicenseControlCenter.war
```

5. Starten Sie die Servertools neu.

Wenn Sie SAP Business One, Version für SAP HANA (Version >= 10.0 FP 2008 und <= 10.0 FP 2108) verwenden und die Komponente Serviceschicht installiert ist, können Sie die Schwachstelle für die Serviceschicht mit der folgenden Vorgehensweise mindern:

1. Wechseln Sie in das Installationsverzeichnis der Servertools (z.B. */usr/sap/SAPBusinessOne*).
2. Navigieren Sie zum Verzeichnis webapps des *ServiceLayer Controller*:

/usr/sap/SAPBusinessOne/ServiceLayer/ServiceLayerController/webapps

3. Führen Sie den folgenden Befehl aus, um die *JndiLookup.class* von *log4j-core-2.7.jar* aus *ServiceLayerController.war* zu entfernen:

```
unzip ServiceLayerController.war WEB-INF/lib/log4j-core-2.7.jar -d.
zip -q -d WEB-INF/lib/log4j-core-2.7.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
zip ServiceLayerController.war WEB-INF/lib/log4j-core-2.7.jar
rm -r WEB-INF
```

4. Stellen Sie die Berechtigung von *ServiceLayerController.war* wieder her, indem Sie den folgenden Befehl ausführen:

```
chown b1service0:b1service0 ServiceLayerController.war
```

5. Starten Sie die Servertools neu.

Wenn Sie SAP Business One, Version für SAP HANA (Version >= 10.0 FP 2105 und <= 10.0 FP2108) verwenden und die Komponente Job Service installiert ist, können Sie die Schwachstelle für den Jobdienst mit der folgenden Vorgehensweise mindern:

1. Wechseln Sie in das Installationsverzeichnis der Server-Tools (z.B. */usr/sap/SAPBusinessOne*)
2. Navigieren Sie zum Verzeichnis webapps *des ReportingService Controller*:

/usr/sap/SAPBusinessOne/ServerTools/ReportingService/webapps

4. Führen Sie den folgenden Befehl aus, um die *JndiLookup.class* von *log4j-core-2.14.0.jar* aus *ReportingService.war* zu entfernen:

unzip ReportingService.war WEB-INF/lib/log4j-core-2.14.0.jar -d.
zip -q -d WEB-INF/lib/log4j-core-2.14.0.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
zip ReportingService.war WEB-INF/lib/log4j-core-2.14.0.jar
rm -r WEB-INF

5. Stellen Sie die Berechtigung von *ReportingService.war* wieder her, indem Sie den folgenden Befehl ausführen:

chown b1service0:b1service0 ReportingService.war

6. Starten Sie die Servertools neu.

Wenn Sie SAP Business One, Version für SAP HANA (Version >= 10.0 FP 2008 und <= 10.0 FP 2108) verwenden und die Komponente Extension Manager (SLD) installiert ist, können Sie die Schwachstelle für Extension Manager wie folgt mindern:

1. Wechseln Sie in das Installationsverzeichnis der Servertools (z.B. */usr/sap/SAPBusinessOne*).
2. Navigieren Sie zum Verzeichnis webapps von *ExtensionManager*:

/usr/sap/SAPBusinessOne/ServerTools/ExtensionManager/webapps

3. Führen Sie den folgenden Befehl aus, um die JndiLookup.class von log4j-core-2.7.jar aus ExtensionManager.war zu entfernen:

unzip ExtensionManager.war WEB-INF/lib/log4j-core-2.7.jar -d.
zip -q -d WEB-INF/lib/log4j-core-2.7.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
zip ExtensionManager.war WEB-INF/lib/log4j-core-2.7.jar
rm -r WEB-INF

4. Stellen Sie die Berechtigung von *ExtensionManager.war* wieder her, indem Sie den folgenden Befehl ausführen:

chown b1service0:b1service0 ExtensionManager.war

5. Starten Sie die Servertools neu.

Wenn SAP Business One Integration Framework (B1 10.0 FP2105 und B1 10.0 FP2108) installiert ist, kann die Schwachstelle für das Integration Framework mit der folgenden Vorgehensweise kompensiert werden:

Option 1: Deaktivieren Sie die Ausführung von Crystal Reports im Integration Framework:

1. Navigieren Sie zu *%InstallationDir%\IntegrationServer\Tomcat\webapps\B1iXcellerator*.
2. Bearbeiten Sie die Datei *xcellerator.cfg*, und ändern Sie *xcl.reporting=false*.
3. Starten Sie *Tomcat* oder *den Integrationsdienst* neu.

Nebeneffekt: Die Reporting-Verarbeitungsfunktion wird deaktiviert.

Option 2:

1. Kopieren Sie *%InstallationDir%\IntegrationServer\Tomcat\webapps\B1iXcellerator\WEB-INF\lib\log4j-core.jar* in ein temporäres Verzeichnis namens *%TempDir%*.
2. Verwenden Sie die Befehlszeile und cd für temp *dir %TempDir%*
3. Führen Sie *> jar -xvf log4j-core.jar aus*, und verschieben Sie die temporäre *Datei log4j-core.jar* in ein anderes Verzeichnis.
4. Go *%TempDir%\org\apache\logging\log4j\core\lookup* and Delete *JndiLookup.class*
5. Verwenden Sie erneut die Befehlszeile und cd für *%TempDir%.*
6. Führen Sie *> jar -cvf log4j-core.jar aus*.
7. *B1i Tomcat/Integrationsdienst* stoppen
8. Kopieren Sie die *Datei log4j-core.jar* aus dem temporären Verzeichnis, und überschreiben Sie die JAR-Datei in *%InstallationDir%\IntegrationServer\Tomcat\webapps\B1iXcellerator\WEB-INF\lib\log4j-core.jar*.
9. *B1i Tomcat/Integrationsdienst* neu starten

Siehe auch

- https://nvd.nist.gov/vuln/detail/CVE-2021-44228 (https://nvd.nist.gov/vuln/detail/CVE-2021-44228)

Schlüsselwörter

Log4J, CVE-2021-44228, B1, Schwachstelle, Fehler

Attribute

Schlüssel	Wert
Originalsprache	Englisch
Kategorie	Vorgehensweise
Priorität	Normal
Freigabestatus	Für Kunden freigegeben

Produkte

SAP Business One 10.0
SAP Business One 10.0, Version für SAP HANA
SAP Business One 9.3
SAP Business One 9.3, Version für SAP HANA

Dieses Dokument bezieht sich auf

SAP-Hinweis/Wissensdatenbankartikel	Titel
3131740	[CVE-2021-44228] Schwachstelle bei Remote Code Execution in Verbindung mit Apache-Log4j-2-Komponente in SAP Business One (https://launchpad.support.sap.com/#/notes/3131740)