3131789 - Mitigate Log4j CVE-2021-44228 Vulnerability in SAP Business One

Version	7	**Typ**	Artikel der SAP Wissensdatenbank
Sprache	Englisch	**Originalsprache**	Englisch
Freigabestatus	Released to Customer	**Kategorie**	How-to
Komponente	SBO-CRO-SEC (Sicherheit in SAP Business One Software)	**Freigegeben am**	13.01.2022

Please find the original document at **https://launchpad.support.sap.com/#/notes/3131789**

Symptom

- Vulnerability CVE-2021-44228 for log4j
- How does this impact SAP Business One
- log4j is an apache library used commonly in java applications. This particular issue was identified in **log4j2** and fixed in log4j 2.15.0.

Umgebung

SAP Business One

Lösung

SAP has provided a feature package addressing this issue as per SAP Note 3131740. Customers need to implement or upgrade to SAP Business One FP2111.

Workaround

Please assess the workaround applicability for your SAP landscape prior to implementation.

Note that this workaround is a temporary fix and is not a permanent solution. SAP strongly recommends to apply the corrections outlined in the security note, which can be done in lieu of the workaround or after the workaround is implemented.

When using SAP Business One or SAP Business One, version for SAP HANA (version >= 9.3 PL07 and <= 10.0 FP2108) and the component Workflow is installed, you can mitigate the vulnerability for Workflow with the following procedure:

1. Open the package *C:\Program Files (x86)\sap\SAP Business One ServerTools\Workflow\workflow-service.war* in winrar. (Right click open in winrar.)
2. Traverse to *\WEB-INF\lib\log4j-core-2.13.3.jar* and remove the *JndiLookup* class from the classpath: *org/apache/logging/log4j/core/lookup/JndiLookup.class.* For version >= 9.3 PL07 and < 10.0 FP2008, traverse to \WEB-INF\lib\log4j-core-2.11.1.jar, and do the operation.
3. Accept the update archive.
4. Restart the *SAP Business One Workflow Engine* from the windows services.

When using SAP Business One (version >= 10.0 FP 2008 and <= 10.0 FP 2108) and the component License Server is installed, you can mitigate the vulnerability for License Server with the following procedure:

1. Open the package *C:\Program Files (x86)\SAP\SAP Business One ServerTools\LicenseHTTPS\webapps\LicenseControlCenter.war* in winrar. (Right click *LicenseControlCenter.war* and open it with winrar).
2. Traverse to *\WEB-INF\lib\log4j-core-2.7.jar* and remove the *JndiLookup* class from the classpath: *org/apache/logging/log4j/core/lookup/JndiLookup.class*.
3. Accept the update archive.
4. Restart the *SAP Business One Server Tools Service* from the windows services.

When using SAP Business One (version >= 10.0 FP 2008 and <= 10.0 FP 2108) and the component Service Layer is installed, you can mitigate the vulnerability for Service Layer with the following procedure:

1. Go to the 64-bit Server Tools installation folder (for example, *C:\Program Files\SAP\SAP Business One ServerTools*).
2. Navigate into the *ServiceLayerController* webapp folder: *.\ServiceLayer\ServiceLayerController\webapps*
3. Right click the *ServiceLayerController.war* and open it with winrar.
4. Traverse to *WEB-INF\lib\log4j-core-2.7.jar*, double-click it and you will see the folder structure of *log4j-core-2.7.jar*.
5. Find the file *JndiLookup.class* from the class path: *org/apache/logging/log4j/core/lookup* and delete this file.
6. Accept the updated archive.
7. Restart the 64-bit *SAP Business One Server Tools Service* from the windows services.

When using SAP Business One (version >= 10.0 FP 2105 and <= 10.0 FP2108) and the component Job Service is installed, you can mitigate the vulnerability for Job Service with the following procedure:

1. Open the package *C:\Program Files (x86)\SAP\SAP Business One ServerTools\ReportingService\webapps\ReportingService.war* in winrar. (Right click open in winrar.)
2. Traverse to *\WEB-INF\lib\log4j-core-2.14.0.jar* and remove the *JndiLookup* class from the classpath: *org/apache/logging/log4j/core/lookup/JndiLookup.class*
3. Accept the update archive.
4. Restart the *SAP Business One Server Tools Service* from the windows services.

When using SAP Business One (version >= 10.0 FP 2008 and <= 10.0 FP 2108) and the component Extension Manager(SLD) is installed, you can mitigate the vulnerability for Extension Manager with the following procedure:

1. Open the package *C:\Program Files (x86)\SAP\SAP Business One ServerTools\ExtensionManager\webapps\ExtensionManager.war* in winrar. (Right click *ExtensionManager.war* and open it in winrar.)
2. Traverse to *\WEB-INF\lib\log4j-core-2.7.jar* and remove the *JndiLookup* class from the classpath: *org/apache/logging/log4j/core/lookup/JndiLookup.class.*
3. Accept the update archive.
4. Restart the *SAP Business One Server Tools Service* from the windows services.

When using SAP Business One, version for SAP HANA (version >= 10.0 FP 2008 and <= 10.0 FP 2108) and the component License Server is installed, you can mitigate the vulnerability for License Server with the following procedure:

1. Go to the server tools installation directory (for example, */usr/sap/SAPBusinessOne*)
2. Navigate into the License's webapps directory:

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

3. Run the following command to remove the *JndiLookup.class* of log4j-core-2.7.jar from *LicenseControlCenter.war*:

```
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. Restore the permission of *LicenseControlCenter.war* by running the following command:

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

5. Restart the server tools.

When using SAP Business One, version for SAP HANA (version >= 10.0 FP 2008 and <= 10.0 FP 2108) and the component Service Layer is installed, you can mitigate the vulnerability for Service Layer with the following procedure:

1. Go to the server tools installation directory (for example, */usr/sap/SAPBusinessOne*)
2. Navigate into the *ServiceLayer Controller*'s webapps directory:

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

3. Run the following command to remove the *JndiLookup.class* of *log4j-core-2.7.jar* from *ServiceLayerController.war*:

```
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. Restore the permission of *ServiceLayerController.war* by running the following command:

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

5. Restart the server tools.

When using SAP Business One, version for SAP HANA (version >= 10.0 FP 2105 and <= 10.0 FP2108) and the component Job Service is installed, you can mitigate the vulnerability for Job Service with the following procedure:

1. Go to the server tools installation directory (e.g. */usr/sap/SAPBusinessOne*)

2. Navigate into the *ReportingService Controller's* webapps directory:

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

4. Run the following command to remove the *JndiLookup.class* of *log4j-core-2.14.0.jar* from *ReportingService.war*:

```
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. Restore the permission of *ReportingService.war* by running the following command

*chown b1service0:b1service0 ReportingService.wa*r

6. Restart the server tools.

When using SAP Business One, version for SAP HANA (version >= 10.0 FP 2008 and <= 10.0 FP 2108) and the component Extension Manager(SLD) is installed, you can mitigate the vulnerability for Extension Manager with the following procedure:

1. Go to the server tools installation directory (for example, */usr/sap/SAPBusinessOne*)
2. Navigate into the *ExtensionManager*'s webapps directory:

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

3. Run the following command to remove the JndiLookup.class of log4j-core-2.7.jar from ExtensionManager.war:

```
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. Restore the permission of *ExtensionManager.war* by running the following command:

chown b1service0:b1service0 ExtensionManager.war

5. Restart the server tools.

When SAP Business One Integration Framework (B1 10.0 FP2105, and B1 10.0 FP2108) is installed, the vulnerability for Integration Framework can be mitigated with the following procedure:

Option 1: Switch off the execution of the Crystal Reports in the integration framework:

1. Go to *%InstallationDir%\IntegrationServer\Tomcat\webapps\B1iXcellerator*.
2. Edit the *xcellerator.cfg* file, and change *xcl.reporting=false*.
3. Restart the *Tomcat* or *Integration Service*.

Side effect: The reporting processing functionality will be disabled.

Option 2:

1. Copy *%InstallationDir%\IntegrationServer\Tomcat\webapps\B1iXcellerator\WEB-INF\lib\log4j-core.jar* to a temp directory, named as *%TempDir%*

2. Use command line, and cd to temp *dir %TempDir%*

3. Run > *jar -xvf log4j-core.jar* and move the temp l*og4j-core.jar* to another dir

4. Go *%TempDir%\org\apache\logging\log4j\core\lookup* and Delete *JndiLookup.class*

5. Use command line, and cd to *%TempDir% again*

6. Run > *jar -cvf log4j-core.jar*.

7. Stop *B1i Tomcat / Integration Service*

8. Copy the *log4j-core.jar* from temp dir and overwrite the jar file in *%InstallationDir%\IntegrationServer\Tomcat\webapps\B1iXcellerator\WEB-INF\lib\log4j-core.jar*

9. Restart *B1i Tomcat / Integration Service*

Siehe auch

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

Schlagwörter

Log4J, CVE-2021-44228, B1, vulnerability, bug

Produkte

SAP Business One 10.0
SAP Business One 10.0, version for SAP HANA
SAP Business One 9.3
SAP Business One 9.3, version for SAP HANA

Dieses Dokument referenziert auf

SAP-Hinweis/KBA	Titel
3131740	[CVE-2021-44228] Schwachstelle bei Remote-Code-Ausführung in Verbindung mit Apache-Log4j-2-Komponente in SAP Business One