

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

Version	1	Type	SAP Knowledge Base Article
Language	English	Master Language	English
Release Status	Released to Customer	Category	How To
Component	SBO-CRO-SEC (Security in SAP Business One software)	Released On	15.12.2021

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.

Environment

SAP Business One

Resolution

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. Go to directory *C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\bin*, back up *tomcat8w.exe* and then rename *tomcat8w.exe* to *B1Workfloww.exe*.
2. Double-click *B1Workfloww.exe* to open *SAP Business One Workflow Engine Properties* form, go to the *Java* tab, add the following content in *Java Options* and save

```
-Dlog4j2.formatMsgNoLookups=true
```

3. Rename *B1Workfloww.exe* back to *tomcat8w.exe*
4. Restart *Workflow Engine Service* 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 \geq 10.0 FP 2008 and \leq 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 \geq 10.0 FP2102 and \leq 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 directory *C:\Program Files (x86)\SAP\SAP Business One ServerTools\Common\tomcat\bin*, back up *tomcat8w.exe* and then rename *tomcat8w.exe* to *B1ServerToolsw.exe*
2. Double-click *B1ServerToolsw.exe* to open *SAP Business One Server Tools Service Properties* form, go to the *Java* tab, add the following content in Java Options and save

-Dlog4j2.formatMsgNoLookups=true

3. Rename *B1ServerToolsw.exe* back to *tomcat8w.exe*.
4. Restart *SAP Business One Server Tools Service* from the windows services.

When using SAP Business One (version \geq 10.0 FP 2008 and \leq 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 \geq 10.0 FP 2008 and \leq 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 \geq 10.0 FP 2008 and \leq 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 \geq 10.0 FP 2102 and \leq 10.0 FP2108) and the component Job Service is installed, you can mitigate the vulnerability for Job Service with the following procedure:

1. Open file */etc/init.d/sapb1servertools*.
2. Change the value of variable 'JAVA_OPTS', add a new option as follows:

```
JAVA_OPTS="$JAVA_OPTS -Duser.country=US -Duser.language=en -Dfile.encoding=UTF-8 -
Djava.awt.headless=true -server -Xms1024m -Xmx5120M -XX:MetaspaceSize=128m -
XX:MaxMetaspaceSize=512m -Dlog4j2.formatMsgNoLookups=true"
```

2. Save and close the file.
3. Restart the server tools.

When using SAP Business One, version for SAP HANA (version \geq 10.0 FP 2008 and \leq 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\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: Add JVM Args to disable Msg Lookups:

1. Go to `%InstallationDir%\IntegrationServer\Tomcat\bin` folder.
2. Execute `tomcat8w.exe`.
3. Go to the *Java* tab.
4. Add `-Dlog4j2.formatMsgNoLookups=true` to the Java options.
5. Restart the *Tomcat* or *Integration Service*.

See Also

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

Keywords

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

Products

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