3129956 - CVE-2021-44228 - BusinessObjects impact for Log4j vulnerability

Version	15	**Type**	SAP Knowledge Base Article
Language	English	**Master Language**	English
Release Status	Released to Customer	**Category**	Problem
Component	BI-BIP-DEP (Webapp Deployment, Networking, Vulnerabilities, Webservices)	**Released On**	14.12.2021

Please find the original document at **https://launchpad.support.sap.com/#/notes/3129956**

Symptom

- Vulnerability CVE-2021-44228 for log4j
- How does this impact SAP BusinessObjects Business Intelligence Platform (BI) 4.x
- 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 BusinessObjects Business Intelligence Platform 4.2, 4.3
- SAP BusinessObjects Business Intelligence (BI) Platform 4.0 / 4.1 *** NO LONGER SUPPORTED**
- SAP Crystal Server 2016, 2020
- SAP Crystal Reports 2016, 2020
- SAP Crystal Reports for Enterprise 4.2, 4.3
- Live Office
- Analysis for Office (AO) and Analysis for Office Add-on for BI Platform
- Lumira Discovery, Lumira Server for BI Platform & Lumira Designer
- SAP BI Mobile server
- All Operating Systems

Resolution

- SAP BusinessObjects BI Platform is **not impacted** by the CVE-2021-44228. This applies to all the SAP BI products listed in the Environment section.
  See: https://support.sap.com/content/dam/support/en_us/library/ssp/my-support/trust-center/sap-tc-01-5025.pdf

Further details (for information purposes only - it does not change the statement above):

- The impacted component is the main JNDI package. **JNDI classes and methods are not used in the SAP BusinessObjects BI Platform**.
- The version of log4j in releases of BI can be determined by opening the log4j.jar file in a zipping tool, and reading the MANIFEST.MF file in META-INF
- The version of Apache Struts included in the platform relies on **log4j-api**, which is also not affected by the vulnerability. Only the module **log4j-core** is affected.
- Further security / mitigation against Remote Code Execution is available at the Java level in 8u121 and

8u191, therefore we recommend customers to be on a version of SAP BusinessObjects BI Platform that packages at least a version > 8u121. Therefore we recommend the **minimum** version that should be applied is 4.2 SP05. For more information about the versions of SAPJVM (and which Oracle JVM version they are based on) supplied per BI version, see:
2914488 - List of Bundled SAP JVM versions shipped with selected Patches of SAP BusinessObjects Business Intelligence Platform 4.x

For more information:

- https://logging.apache.org/log4j/2.x/security.html
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228

For CR4Eclipse / CR4VS, see:

- 3131199 - CVE-2021-44228 - CR4Eclipse / CR4VS impact for Log4j vulnerability

For SAP Data Services / Information Steward, see:

- 3129934 - CVE-2021-44228 - Log4j vulnerability - no impact on SAP EIM products: SAP Data Services, SAP Cloud Integration for Data Services
- 3131007 - CVE-2021-44228 - Log4j vulnerability - no impact on SAP Information Steward

Keywords

CVE-2021-44228, SAP BusinessObjects, 4.3, 4.2, log4j,vulnerability, JNDI

Products

SAP BusinessObjects Business Intelligence platform 4.2
SAP BusinessObjects Business Intelligence platform 4.3

Other Components

Component	Description
BI-BIP-INS	Installation, Updates, Upgrade, Patching

