INDICO SOLUTIONS

CVE-2021-44228 Sicherheitslücke im Java-Logging mit Log4J

Log4J-Fehler und -Patches

Der kritische Zustand in der Bibliothek Log4J betrifft die Version Log4J 2 und ist mit Log4J 2.15 behoben worden. Eine Sicherheitslücke in Folge von Patch 2.15 wurde schließlich am 14.12.2021 mit 2.16 geschlossen. Die Auslieferung von entsprechenden Updates obliegt jedoch nicht nur SAP, sondern auch den Entwicklern von betroffenen Applikationen.

Log4J in Version 1.X ist schon länger aus der Wartung und wurde daher weder gepatcht noch auf eine Sicherheitslücke untersucht.

Generell empfiehlt es sich alle Systeme in Ihrer IT-Landschaft regelmäßig auf den neusten Stand zu bringen.

Informationen zu betroffenen SAP-Lösungen:

Für alle aufgelisteten Produkte gilt, dass eine Untersuchung nur für die aktuellen, in der Wartung befindlichen Versionen durchgeführt wurde.

SAP BO (BI Platform)	Nicht betroffen
SAP Netweaver JAVA	Unter Einschränkungen betroffen (in Abhängigkeit zu den installierten Applikationen)
SAP Cloud Connector	Nicht betroffen
Simple Diagnostics Agent	Nicht betroffen
SAP EIM (SAP Data Services, SAP Cloud Integration for Data Services)	Nicht betroffen
SAP Integration Suite (Open Connectors)	Nicht betroffen
SQL Anywhere	Nicht betroffen
SAP Cloud Integration NEO & CF Apps	Unter Einschränkungen betroffen (in Abhängigkeit zu den angebundenen Inhalten)
SAP Information Steward	Nicht betroffen
CA Wily Introscope EM Server	Nicht betroffen (aktualisiert am 23.12)
Mainframe Connect Client and Server	Nicht betroffen

Tomcat Apache	Betroffen - Applikationen sollten geupdated oder die Umgebung angepasst werden
SAP Replication Server	Nicht betroffen
SAP Liquidity Management Suite	Nicht betroffen
Oracle	Nicht betroffen sind nach Untersuchungen von Oracle: Oracle Database, Oracle Instant Client, Oracle-Exadata-Storage-Server-Software, Oracle Fail safe, Universal Installer
SAP Convergent Charging	Nicht betroffen
SAP Financial Consolidation	Nicht betroffen
Crystal Reports 4 Eclipse	Ist je nach Version betroffen
SAP SDK	Nicht betroffen
R4CM CORWEB JAVA-Adapter (für PO von SOA People)	Betroffen
Sap Mobile Platform Server & Mobile Services	Nicht betroffen
AS Java Enterprise Portal	Unter Einschränkungen betroffen (in Abhängigkeit zu den installierten Applikationen)
SAP BO Financial Information Management	Nicht betroffen
Dell Boomi (Success Factors)	Betroffen
SAP Financial Consolidation Cube Designer	Nicht betroffen
Adaptive Server Enterprise	Nicht betroffen
SAP Litmos Training	Nicht betroffen
SAP Landscape Transformation Replication Server	Nicht betroffen
SAP Online Banking	Unter Einschränkungen betroffen (in Abhängigkeit zu den installierten Drittanbieterprodukten oder Kundenerweiterungen)
SAP Online Retail Banking	Unter Einschränkungen betroffen (in Abhängigkeit zu den installierten Drittanbieterprodukten oder Kundenerweiterungen)
SAP Enterprise Thread Detection & ETD Log Collector	Wird noch untersucht
SAP HANA DB	Betroffen (Aber nur die XS Advanced Runtime)
SAP Predictive Analytics	Nicht betroffen
SAP CM	Unter Einschränkungen betroffen (Abhängig von der Version)
SAP Data Intelligence on-premise	Betroffen
SAP Commerce Platform	Betroffen
SAP ProductAuthority/AuthoritySuite/Lifecycle	Nicht betroffen
SAP HANA Smart Integration	Nicht betroffen
SAP IQ	Nicht betroffen
SAP Cloud Portal on NEO & Cloud Foundry	Nicht betroffen

SAP Commerce Cloud SAP Infrastructure	Betroffen
SAP Commerce Cloud Public Cloud	Betroffen
SAP Content Server <= 650	Nicht betroffen
Universal Worklist	Unter Einschränkungen betroffen (in Abhängigkeit zu den installierten Applikationen)
SAP BO Suite	Nicht betroffen
AS Java UI Theme designer	Unter Einschränkungen betroffen (in Abhängigkeit zu den installierten Applikationen)
SAP SuccessFactors	Betroffen
Introscope	Nicht betroffen
16.12.2021	
SAP Tenant Cloning Tool (SAP BTP API Management)	Betroffen
SAP Enable Now	Wird noch untersucht
SAP Omnichannel Point-of-Sale GK	Unter Einschränkungen betroffen (in Abhängig zu den installierten Komponenten)
SAP 3D Visual Enterprise	Nicht betroffen
ECF	Betroffen
SAP Customer Checkout	Betroffen
SAP Work Manager/ SAP Inventory Manager	Betroffen
SAP Process Orchestration	Betroffen
17.12.2021	
SAP Process Integration	Betroffen
22.12.2021	
SAP BTP Cloud Foundry	Betroffen
SAP Landscape Management	Betroffen
Connected Health Platform 2.0 – Fhirserver	Betroffen
27.12.2021	
SAP Enable Now Manager	Betroffen
Cloud for Customer Lotus Notes PlugIn	Betroffen
SAP Localization Hub, digital compliance service for India	Betroffen
SAP Edge Services On Premise Edition	Betroffen
SAP BTP API Management (Tenant Cloning Tool)	Betroffen
SAP NetWeaver Process Integration	Betroffen
28.12.2021	
XSA cockpit	Betroffen
03.01.2022	
SAP Edge Services Cloud Edition	Betroffen
Adobe LiveCycle Designer 11.0	Betroffen

Software-Lösungen, die in unserer Liste nicht aufgeführt sind, wurden von uns noch nicht auf mögliche Angriffsvektoren untersucht, daher liefert diese Aufzählung keine Gewähr für Vollständigkeit.

Die weitere Entwicklung des Log4J-Problems und Reaktionen von SAP behalten wir im Blick und informieren Sie zeitnah in unseren Meldungen.