**WDB 211124**

**Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)**
**Auswirkungen auf Sage-Produkte**

Die Produkte von Sage sind bis auf **zwei Ausnahmen** nicht von der Sicherheitslücke betroffen.

Dabei handelt es sich um **Sage CRM** und das **Dokumentenmanagement bzw. die Digitale Personalakte**.

Soweit die Komponente in unseren Produkten enthalten ist haben wir in der nachfolgenden Tabelle hinweise erfasst.

| Produkt | Betroffen von CVE-2021-44228 | Details |
|---|---|---|
| Sage 50 Connected (SmartFinder)<br>Sage 50 Handwerk (SmartFinder) | Nein | Das im SmartFinder verwendete ApacheSolr 5.3.1 wird per Default auf die Weise ausgeliefert und installiert, dass es den RollingFileAppender benutzt. Dieser kann technisch keine JNDI Anfragen erstellen. Aus diesem Grund ist der SmartFinder und damit auch Sage50 Connected sowie Sage50 Handwerk von diesen Schwachstellen CVE-2021-44228 & CVE-2021-4104 nicht betroffen. |
| Sage b7 | Nein | Llog4j-1.*.jar wird verwendet aber in der Properties-Datei der JMS Appender über die Eigenschaften ist TopicBindingName oder TopicConnectionFactoryBindingName nicht gesetzt |
| Sage ERP | Nein | Kein Java Technologie Stack |
| Sage 100 | Nein | Kein Java Technologie Stack |
| xRM | Nein | Kein Java Technologie Stack |
| HR Suite | Nein | Kein Java Technologie Stack |
| LohnXL | Nein | Kein Java Technologie Stack |
| Sage Business Cloud Payroll | Nein | Kein Java Technologie Stack |
| SOO | Nein | Kein Java Technologie Stack |
| Sage Wincarat | Nein | Kein Java Technologie Stack |
| X3 | Nein | Wenn die Installation nach den Security Guidelines erfolgt ist, besteht kein Risiko. Falls die Guidelines nicht beachtet wurden, gibt es eine Komponente, die ggf. ein Update erfordert um sie abzusichern. Es handelt sich dabei um Elastic Search und ein Update ist bereits auf der Hersteller Website verfügbar |
| Sage CRM | Ja | Das SageCRM-Team wird für die aktuell unterstützten Versionen Patches liefern. Für folgende Versionen sind sie bereits im Test:<br>Sage CRM 2020 R2<br>Sage CRM 2021 R1<br>Sage CRM 2021 R2<br>Sobald sie verfügbar sind, wird von uns ein WDB-Artikel mit den Downloads veröffentlicht.<br>Quelle (15.12.2021)<br>https://www.sagecity.com/sage-global-solutions/sage-crm/f/sage-crm-announcements-news-and-alerts/178799/advisory-apache-log4j-vulnerability-cve-2021-45046 |

| | | |
|---|---|---|
| OL24 / Sage100 Hosting | Nein | Kein Java Technologie Stack |
| Sage New Classic / SNC Webclient | Nein | Kein Java Technologie Stack |
| Sage Online-Portale (ServiceWelt, PartnerForum, SupportCenter usw.) | Nein | Kein Java Technologie Stack |
| d.velop (S100 DMS, HR DPA) | Ja | In den Desktopprodukten ist kein Tool betroffen, das Sage-seitig genutzt wird.<br><br>Sollte im Folgegeschäft der "Presentation-Server" genutzt werden, müssen kundenindividuell die Webapps der Log4j Bibliothek aktualisiert werden<br>In den Cloudprodukten ist die "Aufgabenverwaltung" betroffen. Bei den Cloudprodukten erfolgt ein automatisches Patch durch d.velop.<br><br>Bei Nutzung des Presatation Servers (z.B. für Workflowengine) muss eine manuelle Anpassung erfolgen. Da es sich hier jedoch nicht um eine Standardkomponente handelt, die im Sage Server Setup genutzt wird, sondern nur bei Folgegeschäft zum Tragen kommt, informieren Sie sich bitte bei d.velop über den folgenden Link: https://kb.d-velop.de/s/article/000001798 |
| TMS Archiv (HR) | Nein | |
| E-Bilanz HSH | Nein | Opti.Tax und entsprechende OEM Client Versionen sind von dieser Java Sicherheitslücke nicht betroffen.<br>Log4j wird von uns nicht verwendet.<br>Es besteht kein Handlungsbedarf. |
| Webshop epages | Nein | Nach jetzigem Stand (14.12.2021) ist der Shop von epages nicht direkt betroffen. Lediglich die Logfile Aggregation mit Logstash und Elasticsearch benutzt die betroffene Bibliothek. Dafür hat epages gestern einen Workaround eingespielt. |
| Sage 50 Handwerk mobile Objects | Nein | Unser Webservice ist nicht von dem Problem betroffen |
| Sage 50 Handwerk Cloud (powered by Loginfinity) | Nein | Kein Java Technologie Stack |