Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)

Auswirkungen auf Sage-Produkte

Die Produkte von Sage sind, bis auf eine Ausnahme, nicht von der Sicherheitslücke betroffen.
Dabei handelt es sich um Sage CRM.
Soweit die Komponente in unseren Produkten enthalten ist haben wir in der Tabelle entsprechende Details und Hinweise erfasst.

Produkt	**Betroffen von** **CVE-2021-44228**	**Details**
Sage 50 Connected (SmartFinder) Sage 50 Handwerk (SmartFinder)	nicht betroffen in unserer Konfiguration	Das im Smartfinder verwendete ApacheSolr 5.3.1 beinhaltet Log4J in der Version 1.2.17. Diese Version ist nicht von der ursprünglichen schwerwiegenden kritischen Schwachstelle CVE-2021-44228 betroffen, welche sich auf die Log4J Versionen 2.0-2.14.1 bezieht. Im Rahmen weiterer Analysen zu CVE-2021-44228 wurde eine etwas geringer kritische Schwachstelle zu Log4J in der Version 1.2.17 entdeckt: CVE-2021-4104. Zu dieser Schwachstelle kommt es allerdings nur dann, wenn ApacheSolr mit einer Logging Konfiguration betrieben wird, die nicht der Standardeinstellung

		entspricht, genauer gesagt, wenn der JMSAppender verwendet wird, um Logeinträge zu erstellen. Dieser kann dann dazu missbraucht werden, um JNDI Anfragen auszulösen die zur gleichen Wirkung wie CVE-2021-44228 führen. 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. Quellen: https://logging.apache.org/log4j/2.x/security.html https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228 https://nvd.nist.gov/vuln/detail/CVE-2021-4104 https://nvd.nist.gov/vuln/detail/CVE-2021-44228
Sage 50 Adressen	Nein	Kein Java Technologie Stack
GS-Verein	Nein	Kein Java Technologie Stack
Sage b7	Nein	Update 4 wurde überprüft verwendet log4j-1.*.jar und in der Properties-Datei der JMS Appender über die Eigenschaften ist TopicBindingName oder TopicConnectionFactoryBindingName nicht gesetzt.
Sage ERP	Nein	(siehe Fremdsysteme) ist nicht direkt betroffen kein Java Technologie Stack
Sage 100	Nein	Keine JAVA Bibliotheken verwendet
xRM	Nein	Keine JAVA Bibliotheken verwendet

HR Suite	Nein	Kein Java Technologie Stack
Sage Business Cloud Payroll	Nein	
LohnXL	Nein	Kein Java Technologie Stack
SOO	Nein	Weder auf dem Gateway noch auf den Web oder Provisioning Server und auch auf den Appservern ist Java nicht installiert.
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: Sage CRM 2020 R2 Sage CRM 2021 R1 Sage CRM 2021 R2 Sobald sie verfügbar sind, wird von uns ein WDB-Artikel mit den Downloads veröffentlicht. Quelle (15.12.2021) 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	nicht betroffen
Sage New Classic / SNC Webclient	Nein	nicht betroffen

Sage Online-Portale (ServiceWelt, PartnerForum, SupportCenter usw.)	Nein	Kein Java Technologie Stack
d.velop (Produkte: Sage X3, Sage b7, Sage Wincarat, Sage 100, Sage HR Suite, Sage ERP, Sage 50 Handwerk)	Nein	Desktopprodukten ist kein Tool betroffen, das Sageseitig genutzt wird. Bei den Cloudprodukten erfolgte ein automatisches Patch seitens d.velop.In den In den Cloudprodukten war die "Aufgabenverwaltung" betroffen. Sollte im Folgegeschäft der "Presentation Server" genutzt werden, müssen kundenindividuell die Webapps der Log4j Bibliothek aktualisiert werden https://kb.d-velop.de/s/article/000001798
TMS Archiv (HR)	Nein	System ist nicht betroffen
E-Bilanz HSP	Nein	Opti.Tax und entsprechende OEM Client Versionen sind von dieser Java Sicherheitslücke nicht betroffen. Log4j wird nicht verwendet. Es besteht kein Handlungsbedarf. Folgenden Beitrag hat HSP zu diesem Thema veröffentlicht: Schwachstelle Java-Bibliothek (Log4j)
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 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
finleap connect (Sage ERP)	Nein	Es wird keine Java Technologie genutzt.