Sicherheitshinweis: DocuWare und log4J2 Sicherheitslücke [DW-2021-0001.2]

- Ausgabedatum: 14.12.2021
- Aktualisiert am: 15.12.2021
- CVE(s): CVE-2021-44228, CVE-2021-45046

Zusammenfassung

Eine Open-Source-Bibliothek, die in vielen Produkten weltweit eingesetzt wird, weist eine schwere Sicherheitslücke auf: **Apache log4j2**

Die offizielle Dokumentation zu dieser Sicherheitslücke finden Sie hier:

- https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce
- https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3

Zusammenfassend lässt sich sagen, dass die Nutzung von DocuWare in der Cloud und On-Premises **nicht** (mehr) von dieser Sicherheitslücke betroffen ist. Weitere Details und Empfehlungen finden Sie unten.

Nicht betroffene DocuWare Produkte

Der größte Teil der DocuWare Produkte verwendet überhaupt kein Java und ist daher nicht von CVE-2021-44228 betroffen. Einige wenige Produktteile verwenden die betroffene Bibliothek, sind aber nicht oder nicht mehr betroffen, wie folgt.

DocuWare Cloud 7.4 / 7.5 – Intelligent Indexing und Volltext

DocuWare Cloud wurde analysiert und neu konfiguriert, so dass DocuWare Cloud seit dem 12.12.2021, 08:40 CEST, sicher vor Angriffen von CVE-2021-4428 ist.

Wir haben keinen Grund zu der Annahme, dass die Sicherheitsschwachstelle ausgenutzt wurde. Um auf der sicheren Seite zu sein, wurde die gesamte potenziell betroffene Infrastruktur am 13.12.2021 in einen garantiert sauberen Zustand versetzt.

On-Premises: DocuWare Intelligent Indexing Version 1

Intelligent Indexing Version 1 ist nicht anfällig für CVE-2021-4428, da Eingaben, die an Intelligent Indexing gesendet werden, verarbeitet und nicht direkt von log4j protokolliert werden. Dies wurde von DocuWare getestet und bestätigt.

On-Premises: DocuWare Intelligent Indexing Version 2 (unter Verwendung von Docker Images)

Intelligent Indexing v2 ist nicht anfällig für CVE-2021-4428, da die an Intelligent Indexing gesendeten Eingaben verarbeitet und nicht direkt von log4j protokolliert werden. Dies wurde von DocuWare getestet und bestätigt.

On-Premises – DocuWare Volltext-Server

Der standardmäßige DocuWare Volltext Server verwendet Apache SOLR 4.9.1 und damit auch indirekt die log4j-Bibliothek. Darüber hinaus verwendet er Apache Tomcat 8.0 / 9.0, der jedoch standardmäßig nicht log4j verwendet.

- Die Version von SOLR – einschließlich der Version von eingebettetem log4j 1.2.17 – ist jedoch nicht anfällig für CVE-2021-4428.
    - Anmerkung: Log4j 1.2.17 hat jedoch eine bekannte Schwachstelle (CVE-2019-17571) – diese ist jedoch in unserer Standardkonfiguration, die durch unser Standard-Server-Setup eingerichtet wurde, nicht ausnutzbar. Stellen Sie sicher, dass Sie „org.apache.log4j.net.SocketServer" nicht so konfiguriert haben, dass er auf ungeschützte Netzwerke hört, falls Sie Tomcat selbst eingerichtet haben.

Betroffene DocuWare Produkte

Uns ist nicht bekannt, dass noch DocuWare Produkte betroffen sind.

Aktualisierung bezüglich CVE-2021-45046

Es sind keine DocuWare Produkte von CVE-2021-45046 betroffen.

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046

Die beschriebenen Konfigurationen werden in DocuWare Produkten nicht verwendet.

Allgemeine Empfehlungen

Selbst für den unwahrscheinlichen Fall, dass sich eines der oben genannten Analyseergebnisse als falsch erweist, empfehlen wir zur Sicherheit die folgenden Maßnahmen:

- Die folgende Umgebungsvariable sollte auf allen DocuWare Servern, auf denen DocuWare Volltext läuft, auf Systemebene (nicht auf Benutzerebene) gesetzt werden: LOG4J_FORMAT_MSG_NO_LOOKUPS=true
- Upgrade der Tomcat-Version auf die neueste Minor-Version 9.x (9.0.56) gemäß https://support.docuware.com/de-de/knowledgebase/article/KBA-36103
- Blockieren Sie auf der Firewall den vom Webserver ausgehenden Datenverkehr (wenn das nicht möglich ist, protokollieren und überwachen Sie die vom Webserver initiierten Verbindungen).