Sicherheitslücke im Logging-Framework Log4j
(CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 und CVE-2021-44832)

Das Folgende beschreibt die Möglichkeiten zum Schließen der sehr kritischen Sicherheitslücke CVE-2021-44228 im **contract***manager²*. Neben einem Update ist auch eine manuelle Korrektur möglich. Das konkrete Verfahren ist von der aktuell eingesetzten **contract***manager²*-Version abhängig.

Die nachträglich erkannten, tlw. ebenfalls als kritisch eingestufte Sicherheitslücken CVE-2021-45046 und CVE-2021-45105 werden ebenfalls durch unten beschriebene Maßnahmen korrigiert. Diese Sicherheitslücken basieren im Wesentlichen auf Schwachstellen bei speziellen Logging-Patterns (Context-Lookup, z.B. $${ctx:loginId}), die im **contract***manager²* nicht genutzt werden.

Über die Sicherheitslücke CVE-2021-44832 ist das Einschleusen von Schadcode über spezielle JDBC-Appender möglich, wenn der Angreifer Kontrolle über die Log4j-Konfiguration hat. In der Standard-Konfiguration nutzt der **contract***manager²* solche Appender nicht.

contract*manager²*-Version <= 2.27

Aktualisierung contract*manager²*

Möglichkeit 1 (nur zur Korrektur von CVE-2021-44228): Update auf **contract***manager²* 2.27.6069

- Update herunterladen von unserer FTP-Seite (bitte kontaktieren Sie uns für Zugangsdaten)
- Normale Update-Installation ausführen
- Um auch die Sicherheitslücken CVE-2021-45046, CVE-2021-45105 und CVE-2021-44832 zu schließen, ist ein manueller Austausch der log4j-Bibliotheken nach dem Update erforderlich (s. Möglichkeit 2)

Möglichkeit 2: Manueller Austausch der log4j-Bibliotheken

- Alle contractmanager-Dienste auf dem Server beenden
- Herunterladen der aktuellen Log4j-Bibliotheken (Version 2.17.1) von https://logging.apache.org/log4j/2.x/download.html (Datei apache-log4j-2.17.1-bin.zip) oder nur die für den **contract***manager²* notwendigen Dateien aus unserem Kundenportal (https://www.contractmanager.de/files/contractmanager/media/Download/contractmanager_log4j.zip)
- Folgende Dateien austauschen, im Unterordner lib\java der **contract***manager²*-Installation (Linux: lib/java):
    - log4j-1.2-api-2.*.jar durch log4j-1.2-api-2.17.1.jar
    - log4j-api-2.*.jar durch log4j-api-2.17.1.jar
    - log4j-core-2.*.jar durch log4j-core-2.17.1.jar
- Alle contractmanager-Dienste auf dem Server wieder starten

Aktualisierung Solr-Server (falls die Volltextsuche im Einsatz ist)

Nicht notwendig. Die verwendeten Solr-Versionen 6.6.0 bzw. 7.2.1 nutzen noch Log4j 1.2.17 mit der Standard-Logging-Konfiguration (ohne JMS-Appender / JNDI). Deshalb sind diese Versionen nicht von der Sicherheitslücke betroffen (s. https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228)

contract*manager²*-Version >= 2.28

Aktualisierung contract*manager²*

Möglichkeit 1: Update auf die aktuelle **contract***manager²*-Version (nicht mehr notwendig, falls Sie bereits die am 20.12.2021 veröffentlichte Version 2.32.6092 oder eine neuere einsetzen)

- Update aus dem Download-Bereich der contractmanager-Webseite (https://www.contractmanager.de/login.html) herunterladen
- Normale Update-Installation ausführen
- Falls die Volltextsuche lizenziert und im Einsatz ist, dort die Bibliotheken manuell austauschen (s.u.)

Möglichkeit 2: Manueller Austausch der log4j-Bibliotheken

- Alle contractmanager-Dienste auf dem Server beenden
- Herunterladen der aktuellen Log4j-Bibliotheken (Version 2.17.1) von https://logging.apache.org/log4j/2.x/download.html (Datei apache-log4j-2.17.1-bin.zip) oder nur die für den **contract***manager²* notwendigen Dateien aus unserem Kundenportal (https://www.contractmanager.de/files/contractmanager/media/Download/contractmanager_log4j.zip)
- Folgende Dateien austauschen, im Unterordner lib\java der **contract***manager²*-Installation (Linux: lib/java):
    - log4j-1.2-api-2.*.jar durch log4j-1.2-api-2.17.1.jar
    - log4j-api-2.*.jar durch log4j-api-2.17.1.jar
    - log4j-core-2.*.jar durch log4j-core-2.17.1.jar
- Falls Sie die **contract***manager²*-API einsetzen oder die cm2go-App nutzen, müssen auch die REST-Server im Tomcat aktualisiert werden. Tauschen Sie dazu folgende Dateien aus:
    - Für cm²-API im Unterordner tomcat\webapps\cm2api\WEB-INF\lib der **contract***manager²*-Installation:
        - log4j-web-2.*.jar durch log4j-web-2.17.1.jar
    - Für cm2go-App im Unterordner tomcat\webapps\cm2go\WEB-INF\lib der **contract***manager²*-Installation:
        - log4j-web-2.*.jar durch log4j-web-2.17.1.jar
- Falls auch die Volltextsuche lizenziert und im Einsatz ist, auch hier die Bibliotheken austauschen (s.u.)
- Alle contractmanager-Dienste auf dem Server wieder starten

Aktualisierung Solr-Server (falls die Volltextsuche lizenziert und im Einsatz ist)

Manueller Austausch der log4j2-Bibliotheken (auch nach einem Update auf die neueste **contract***manager²*-Version notwendig!)

- Herunterladen der aktuellen Log4j2-Bibliotheken (Version 2.17.1) von https://logging.apache.org/log4j/2.x/download.html (Datei apache-log4j-2.17.1-bin.zip) oder nur die für den **contract***manager²* notwendigen Dateien aus unserem Kundenportal (https://www.contractmanager.de/files/contractmanager/media/Download/contractmanager_log4j.zip)
- Alle contractmanager-Dienste auf dem Server beenden
- Die Pfade der auszutauschenden Dateien sind abhängig vom Betriebssystem des Servers Unter Windows:
    - in Unterordner solr\server\lib\ext der **contract***manager²*-Installation:
        - log4j-1.2-api-2.*.jar durch log4j-1.2-api-2.17.1.jar
        - log4j-api-2.*.jar durch log4j-api-2.17.1.jar
        - log4j-core-2.*.jar durch log4j-core-2.17.1.jar
        - log4j-slf4j-impl-2.*.jar durch log4j-slf4j-impl-2.17.1.jar
        - log4j-web-2.*.jar durch log4j-web-2.17.1.jar

Unter Linux:

- in Ordner /opt/solr-8.6.2/server/lib/ext:
  - log4j-1.2-api-2.*.jar durch log4j-1.2-api-2.17.1.jar
  - log4j-api-2.*.jar durch log4j-api-2.17.1.jar
  - log4j-core-2.*.jar durch log4j-core-2.17.1.jar
  - log4j-slf4j-impl-2.*.jar durch log4j-slf4j-impl-2.17.1.jar
  - log4j-web-2.*.jar durch log4j-web-2.17.1.jar

- Alle contractmanager-Dienste auf dem Server wieder starten