Sicherheitslücke Log4Shell

Software-Portfolio der DSC Software AG

Karlsruhe, den 14. Dezember 2021

In der Java-Bibliothek Apache Log4j wurde die Sicherheitslücke Log4Shell öffentlich gemacht.

Betroffen von dieser Sicherheitslücke ist Apache Log4j in den Versionen 2.0 bis 2.14.1. Die Sicherheitslücke ist mit der Version 2.15.0 geschlossen worden.

Als vertrauensvoller Partner unserer Kunden informieren wir Sie offiziell zu der Verwendung der Bibliothek Log4j in den Software-Produkten der DSC Software AG.

Wir haben das gesamte DSC-Portfolio der Standard-Software-Produkte analysiert.
Projekt- oder kundenspezifische Entwicklungen sind von dieser Analyse ausgenommen.

Folgender Sachverhalt bzgl. des DSC-Portfolios ist dabei relevant:

- Log4j wird im ECTR-Umfeld **nicht eingesetzt**.
- Log4j wird in unserem FCTR-Umfeld **nicht eingesetzt**.
- Log4j wird in unserem Cloud-Portfolio lediglich in ++monitoring **direkt eingesetzt**.
  - Es wurde ein **Patch** für ++monitoring zur Verfügung gestellt.
  - Elasticsearch, welche bei CROSS·POINT als Drittanbieter-Software eingesetzt wird, verwendet Log4j. Hier empfehlen wir, die **Konfigurationsoption** *log4j2.formatMsgNoLookups* zu setzen.
- Log4j wird in unserem Add-On-Portfolio **nicht direkt eingesetzt**.
  - Die beiden Infrastruktur-Add-Ons ++proFile und ++proCache benötigen Jetty oder einen anderen Servlet- / JSP-Container.
  - In Jetty oder einem anderen Servlet- / JSP-Container kann evtl. Log4j verwendet werden.
- Log4j wird in unserem Integrationsportfolio **nicht eingesetzt**.

Mit vertrauensvollen Grüßen

Dominik Maier
SVP Products & Development, Prokurist

Weitere Informationen des Bundesamts für Sicherheit in der Informationstechnik >