Security vulnerability Log4Shell

Software portfolio of DSC Software AG

Karlsruhe, December 14, 2021

A security vulnerability regarding the Apache Log4j Java library has been communicated.

Apache Log4j is affected by this vulnerability in versions 2.0 to 2.14.1. The vulnerability has been resolved with version 2.15.0.

As a trusted partner of our customers, we officially inform you about the use of the Log4j library in the software products of DSC Software AG.

We have analyzed the entire DSC portfolio of standard software products.
Project-specific or customer-specific developments are excluded from this analysis.

The following is relevant regarding the DSC portfolio:

- Log4j is **not used** in the ECTR environment.
- Log4j is **not used** in the FCTR environment.
- In our cloud portfolio, Log4j is **only used directly** in ++monitoring.
  - A **patch** for ++monitoring has been made available.
  - Elasticsearch, which is used in CROSS-POINT as a third party software, uses Log4j. We recommend setting the configuration option *log4j2.formatMsgNoLookups*.
- Log4j is **not used** directly in our add-on portfolio.
  - Both infrastructure add-ons ++proFile and ++proCache require Jetty or another servlet / JSP container.
  - In Jetty or another servlet / JSP container, Log4j may be used possibly.
- Log4j is **not used** in our integration portfolio.

Trustful regards

Dominik Maier
SVP Products & Development, Authorized Signatory