Security Advisory: DocuWare and log4J2 vulnerability [DW-2021-0001.1]

- Issue Date: 14-DEC-2021
- Updated on: -
- CVE(s): CVE-2021-44228

Summary

An open-source library used widely in many products worldwide has been reported to have a severe vulnerability: **Apache log4j2**

Official documentation about this vulnerability can be found here:

- 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

In summary, usage of DocuWare Cloud or DocuWare as on-premises system is **not** (anymore) affected from this vulnerability. Find more details and recommendations below.

Not impacted DocuWare Products

The biggest part of the DocuWare product suite is not using Java at all and is therefore not affected from CVE-2021-44228. A few product parts use the affected library, but they were not or are no longer affected, as follows.

DocuWare Cloud 7.4 / 7.5 – Intelligent Indexing and Full-text

DocuWare Cloud has been analyzed and re-configured. Since 12-DEC-2021 08:40 CEST DocuWare Cloud is safe from attacks targeting CVE-2021-4428.

We have no reason to believe that the security vulnerability was exploited. To be on the safe side, all potentially impacted infrastructure was re-initialized to a guaranteed clean state on 13-DEC-2021.

On-premises: DocuWare Intelligent Indexing version 1

Intelligent Indexing version 1 is not vulnerable to CVE-2021-4428, as input sent to Intelligent Indexing is parsed and not directly logged by log4j. This was tested and verified by the DocuWare.

On-premises: DocuWare Intelligent Indexing version 2 (using Docker Images)

Intelligent Indexing version 2 is not vulnerable to CVE-2021-4428, as input sent to Intelligent Indexing is parsed and not directly logged by log4j. This was tested and verified by the DocuWare.

On-premises – DocuWare Full-text server

The default DocuWare Full-text server uses Apache SOLR 4.9.1 and thus also using log4j library indirectly. In addition, it uses Apache Tomcat 8.0/9.0, which does not use log4j by default.

- The version of SOLR - including the version of embedded log4j 1.2.17 – is not vulnerable to CVE-2021-4428
    - Side note: Log4j 1.2.17 has a separate known vulnerability (CVE-2019-17571) – but this is not exploitable in our default configuration set up by our standard server setup. If you set up Tomcat on your own, make sure, that you did not configure “org.apache.log4j.net.SocketServer” to listen on unprotected networks.

Impacted DocuWare Products

We are not aware of any other impacted DocuWare products.

General Recommendations

To be entirely safe (in the unlikely case that any of the analysis results above might turn out to be incorrect) we recommend the following mitigations:

- The following environment variable should be set on system (not user) level on all DocuWare servers that run DocuWare Full-text server: LOG4J_FORMAT_MSG_NO_LOOKUPS=true
- Upgrade of the tomcat version to the latest minor version 9.x (9.0.56) according to: https://support.docuware.com/de-de/knowledgebase/article/KBA-36103
- Block on Firewall outgoing traffic initiated by your web server (if it’s not possible then log and monitor connections initiated by the Web server)