VULNERABILITY LOG4SHELL VERSION 2

Analysis result, recommendations and instructions

- Security gap in Java log4j library
- Affected PCS products
- Securing the INTUS COM HTTPS server
- Analysis and recommendations

The German Federal Office for Information Security (BSI) has published a notice about a critical vulnerability in the Java log4j library.

We have already informed you how to use the system property log4j2.formatMsgNoLookups to quickly minimize the risk. Further research by the Apache Software Foundation has shown that it is necessary to update to log4j version 2.17.1 to completely eliminate the risk. If you have already performed the first recommended action, this does not need to be reversed.

As already communicated, the Java log4j library is included in the HTTPS server of INTUS COM 3.4 and INTUS COM 3.5. We provide - as recommended by the Apache Software Foundation (https://logging.apache.org/log4j/2.x/security.html) – an updated jar file including the secure log4j library version 2.17.1 for replacement in your system. This jar file and the instructions for replacing this file are available for download. You can also find it in the PCS Support Center.

Deeper analysis has shown that the DEXICON 5.4 components themselves do not contain the security-critical log4j core library. However, DEXICON always includes INTUS COM. Only for DEXICON installations with versions 5.1 to 5.4 it should be noted that the INTUS COM HTTPS server could be installed as an optional component. We therefore recommend that customers with DEXICON versions 5.1 to 5.4 check whether the INTUS COM HTTPS server has actually been installed. In this case, we also recommend replacing the jar file in your system.

Patches for the current versions of DEXICON and INTUS COM are available since 22/01/12 - as already announced - which contain the secure log4j with version 2.17.1. These will be the versions DEXICON 5.4.4 and INTUS COM 3.5.3. With the installation of these versions the upgrade to the log4j library version 2.17.1 is done automati-cally and the security gap is reliably closed.

In general, we would like to inform you as quickly and transparently as possible. We have created a complete list of PCS software products, which shows which products/product versions are verified safe or affected, including recommended solutions. This list is also available for download and in the PCS Support Center. With regard to third-party applications, we are in close coordination with the respective manufacturers. We update this list regularly according to the current state of knowledge.

On page 2 you will find the step-by-step instructions for the replacement of the jar file.

Replace INTUS COM HTTPS-Server jar-File:

1. Stop INTUSCOM HTTPS server service.
2. Rename the <installation path>\Intuscom\bin\https_server\ https_server.jar file (e.g. https_server.jar.alt) or delete it.

   (Default installation path="C:\Program Files (x86)\PCS-Systemtechnik").
3. Copy the new https_server.jar into the directory <installation path>\Intuscom\https_server\.
4. Rename the <installation path>\Intuscom\doku\ReleaseNotes\rn_https_server.txt file (e.g.rn_https_server.txt.alt) or delete it.
5. Copy the rn_https_server.txt file to the<installation path>\Intuscom\doku\ReleaseNotes\ directory.
6. Start INTUSCOM HTTPS server service.
7. Check the version (INTUSCOM HTTPS server 1.0.8) on the configuration and status window.

PCS Systemtechnik GmbH · Pfälzer-Wald-Str. 36 · 81539 Munich · Tel. +49 89 68004 – 0
Ruhrallee 311 · 45136 Essen · Tel. +49 201 89416 – 0
intus@pcs.com · www.pcs.com