INFO PAPER

PCS PRODUCTS LIST

Analysis and recommendations

Product/Product version	Analysis result	Current recommendation
Older versions of DEXICON Enterprise (before 5.1.0)	No version includes the affected log4j library.	Is safe. No need for action.
DEXICON Enterprise 5.1.0-5.3.1 INTUS COM HTTPS-Server 1.0.4: log4j 2.10.0	In these versions, an INTUS COM HTTPS server with the affected log4j library has been included and installed if necessary.	We recommend checking whether the INTUS COM HTTPS server has actually been installed. In this case, we recommend replacing the jar file in your system. As soon as available we recommend to install the update to DEXICON 5.4.4.
DEXICON Enterprise 5.4.0 -5.4.2 INTUS COM HTTPS-Server 1.0.5: log4j 2.13.3	In these versions, an INTUS COM HTTPS server with the affected log4j library has been included and installed if necessary.	We recommend checking whether the INTUS COM HTTPS server has actually been installed. In this case, we recommend replacing the jar file in your system. As soon as available, we recommend installing the DEXICON 5.4.4 patch.
Older software versions of INTUS COM (vor 3.4.0)	No version includes the affected log4j library.	Is safe. No need for action.
INTUS COM 3.4.0 INTUS COM 3.4.0 HTTPS-Server 1.0.3: log4j 2.10.0	In these versions, an INTUS COM HTTPS server with the affected log4j library has been included and installed if necessary.	We recommend checking whether the INTUS COM HTTPS server has actually been installed. In this case, we recommend replacing the jar file in your system. As soon as available, we recommend updating to INTUS COM 3.5.3.
INTUS COM 3.4.2 INTUS COM 3.4.2 HTTPS-Server 1.0.4: log4j 2.10.0	In these versions, an INTUS COM HTTPS server with the affected log4j library has been included and installed if necessary.	We recommend checking whether the INTUS COM HTTPS server has actually been installed. In this case, we recommend replacing the jar file in your system. As soon as available we recommend to install the update to INTUS COM 3.5.3.
INTUS COM 3.5.0 INTUS COM 3.5.0 HTTPS-Server 1.0.5: log4j 2.13.3	In these versions, an INTUS COM HTTPS server with the affected log4j library has been included and installed if necessary.	We recommend checking whether the INTUS COM HTTPS server has actually been installed. In this case, we recommend replacing the jar file in your system. As soon as available, we recommend installing the INTUS COM 3.5.3.
INTUS COM 3.5.1 INTUS COM 3.5.1 HTTPS-Server 1.0.5: log4j 2.13.3	In these versions, an INTUS COM HTTPS server with the affected log4j library has been included and installed if necessary.	We recommend checking whether the INTUS COM HTTPS server has actually been installed. In this case, we recommend replacing the jar file in your system. As soon as available, we recommend installing the INTUS COM 3.5.3. patch
INTUS Remote Setup	No version includes the affected log4j library.	Is safe. No need for action.
INTUS Remote Conf	It is falsely detected by log4j name search tools. No version includes the affected log4j library.	Is safe. No need for action.
INTUS PS Setup	No version includes the affected log4j library.	Is safe. No need for action.
INTUS PS SE	No version includes the affected log4j library.	Is safe. No need for action.
INTUS Enroll	No version includes the affected log4j library.	Is safe. No need for action.
INTUS E&D	No version includes the affected log4j library.	Is safe. No need for action.
INTUS TPI-Control	No version includes the affected log4j library.	Is safe. No need for action.
INTUS Access ND	No version includes the affected log4j library.	Is safe. No need for action.

Time for security.

Third-party software

Product/Product version	Analysis result	Current recommendation
Software		
ARH	No version includes the affected log4j library.	Is safe. No need for action.
Cayuga R15 Cayuga R16 Cayuga R17	These versions include the affected log4j library.	We recommend to install the latest patches. Cayuga R15: 6.15.1*_19.zip Cayuga R16: 6.16.1*_12.zip Cayuga R17: 6.17.1*_04.zip
Clex SCT	No version includes the affected log4j library.	Is safe. No need for action.
ID.office	No version includes the affected log4j library.	Is safe. No need for action.
ID.office 360	No version includes the affected log4j library.	Is safe. No need for action.
ID.works	No version includes the affected log4j library.	Is safe. No need for action.
INTUS FTC	No version includes the affected log4j library.	Is safe. No need for action.
Janitor	No version includes the affected log4j library.	Is safe. No need for action.
NumberOK Lite	No version includes the affected log4j library.	Is safe. No need for action.
UniC10	No version includes the affected log4j library.	Is safe. No need for action.
Visit	No version includes the affected log4j library.	Is safe. No need for action.

Hardware

AXIS Firmware	No version includes the affected log4j library.	Is safe. No need for action.
HIKVISION Firmware	No version includes the affected log4j library.	Is safe. No need for action.
INTUS Device Firmware	No version includes the affected log4j library.	Is safe. No need for action.
INTUS Flex Firmware	No version includes the affected log4j library.	Is safe. No need for action.
INTUS PegaSys Firmware	No version includes the affected log4j library.	Is safe. No need for action.
Raytech Firmware	No version includes the affected log4j library.	Is safe. No need for action.

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