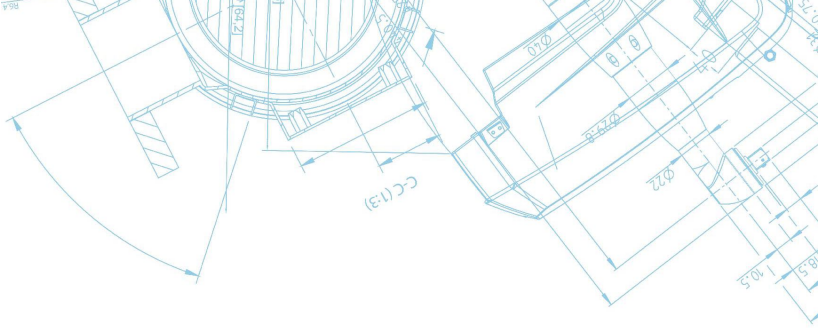

Atlas Copco Tools Central Europe GmbH · Postfach 10 02 44 · D 45002 Essen

All customers

Essen, 14.12.2021

CVE-2021-44228

Dear Sir / Madam,

the cybersecurity issue CVE-2021-44228 in the log4j library is currently affecting a lot of software solutions worldwide. The software products of Atlas Copco are only mildly impacted by this issue, as far as we know yet.

Products/components **not affected**:

- All controller types
- Smart AMS (all versions)
- SQS3 (all versions); this includes the result data viewer SFO 1.x with all its components
- Production Analyzer
- QS-Loop
- ToolsNet 8 (all versions)
- ToolsNet 4000 (all versions)
- Alture
- TechCoverConnect
- Customized solutions (Application Center)
- ToolsTalk 2 (all versions)
- ToolsTalk (older versions)

Products/components **that are affected**:

- Error Proofing License Manager and SQS3 License Manager
- All QA Supervisor versions prior to 06.02e and 06.03a are affected

Atlas Copco Tools Central Europe GmbH

Atlas Copco Tools
Central Europe GmbH
Langemarckstraße 35
45141 Essen
Postfach:
10 02 44, 45002 Essen

Telefon: +49 (0)201 2177 0
Telefax: +49 (0)201 2177 100
tools.de@de.atlascopco.com
www.atlascopco.de

Bankverbindung:
SEB AG
IBAN:
DE76 5122 0200 0030 3510 02
BIC: ESSEDEFFXXX

Geschäftsführer:
Thomas Hülsmann
Olaf Sommer
Claus Schiedek
Peter Edmonds
HRB Essen 5096
UID: DE811155641
St.-Nr.: 111/5706/0482

Our recommendation for the affected product is:

Error Proofing License Manager

Mitigation:

Only the web UI front-end of the License Manager uses the log4j library. It can be disabled without impacting Smart AMS or SQS3 functionality. Both products will still be able to fetch or return feature licenses from the License Manager. Only the management of new and existing feature licenses will not be possible while the UI is disabled.

Please follow the instruction below on how to temporarily disable the web UI of the License Manager. We will provide an updated version of the Error Proofing License Manager as soon as possible.

LINK to Disabling license manager web UI.pdf

QA Supervisor

To change the system configuration of QA Supervisor and close this issue, please follow the instruction in the pdf, link below.

LINK to QA Supervisor Service Procedure XX - Log4j vulnerability CVE-2021-44228.pdf

If you need any support or in case of question, don't hesitate to contact us via:

communications.tools@atlascopco.com

Atlas Copco Tools Central Europe GmbH