



An alle Kunden

14.12.2021

## **CVE-2021-44228**

Sehr geehrte Damen und Herren,

die Sicherheitslücke CVE-2021-44228 in der log4j-Bibliothek betrifft derzeit eine Vielzahl von Softwarelösungen weltweit. Die Softwareprodukte von Atlas Copco sind, soweit wir zum jetzigen Zeitpunkt wissen, nur in geringem Maße von diesem Problem betroffen.

Produkte/Komponenten, die **nicht betroffen** sind:

- Alle Arten von Controllern
- Smart AMS (alle Versionen)
- SQS3 (alle Versionen); einschließlich SFO 1.x mit all seinen Komponenten
- Production Analyzer
- QS-Loop
- ToolsNet 8 (alle Versionen)
- ToolsNet 4000 (alle Versionen)
- Altire
- TechCoverConnect
- Kundenspezifische Lösungen des Application Centers
- ToolsTalk 2 (alle Versionen)
- ToolsTalk (ältere Versionen)

Produkte/Komponenten, **die betroffen sind**:

- Lizenzmanager zum Error Proofing und zur SQS3
- Alle QA-Supervisor-Versionen vor dem Stand 06.02e und 06.03a

Wir empfehlen für die betreffenden Produkte die Umsetzung folgender Maßnahmen:

## **Error Proofing – Lizenzmanager**

Abstellung bis zur Auslieferung eines Updates:

Lediglich das Web-UI-Frontend des Lizenzmanagers verwendet die log4j-Bibliothek. Sie kann deaktiviert werden, ohne die Funktionalität von Smart AMS oder SQS3 zu beeinträchtigen. Beide Produkte sind weiterhin in der Lage, Funktionslizenzen vom Lizenzmanager abzurufen oder zurückzugeben.

Allerdings ist die Verwaltung neuer und bestehender Feature-Lizenzen nicht möglich, solange die Benutzeroberfläche deaktiviert ist.

Bitte befolgen Sie die nachstehende Anleitung zur vorübergehenden Deaktivierung der Web-Benutzeroberfläche des Lizenzmanagers. Wir werden so bald wie möglich eine aktualisierte Version des Lizenzmanagers zum Error Proofing bereitstellen.

Wir kommen ungefragt auf Sie zu, sobald diese bereitsteht

**[LINK zur Deaktivierung des Lizenzmanagers Web-UI.pdf](#)**

## **QA Supervisor**

Um die Systemkonfiguration von QA Supervisor zu ändern und dieses Problem zu beheben, folgen Sie bitte den Anweisungen im untenstehenden PDF-Link.

**[LINK to QA Supervisor Service Procedure XX - Log4j vulnerability CVE-2021-44228.pdf](#)**

Für Rückfragen und sofern Sie Hilfe bei der Umsetzung der Anweisungen benötigen, stehen wir Ihnen gerne zur Verfügung.

**[communications.tools@atlascopco.com](mailto:communications.tools@atlascopco.com)**

Atlas Copco