Brüel & Kjær Vibro
A member of the NSK Group

Dear customer,

Brüel & Kjær Vibro is aware of a security vulnerability identified in CVE-2021-44228. This vulnerability is being referred to as log4jShell and is reported to be under active exploitation.

Immediately upon learning of this vulnerability, Brüel & Kjær Vibro initiated its cyber response plans to identify and mitigate potential risks both within its own environment and within its products.

According to sources, there are two root causes for the log4j vulnerability to appear on a system:

- presence of log4j versions between 2.0 and 2.14.1. All 2.x versions before 2.15.0 are affected.
- presence of Java versions lower than 6u211, 7u201, 8u191, and 11.0.1

After internal investigations we came to the following conclusions:

Condition Monitoring EDGE devices:

- None of our actual Condition Monitoring Devices DDAU *II*, DDAU *III*, VCM-3, VC-6000 or VC-8000 are using any of the impacted software libraries.

Condition Monitoring Diagnostic tools:

Compass Software

- Compass software does **not** use any of the affected libraries. However, Compass software does use Microsoft SQL. Per default Microsoft SQL doesn’t install Java

SQL Server (on Windows) – all editions

- Note: If a customer installs Java support and deploys Java Archives (JARs) that depend on the Log4j 2 library, they are advised to either upgrade to the latest version or remove the Java Archives (JARs) that require the dependency.
-

Vibrosuite software

- Vibrosuite software does **not** use any of the affected libraries. However, Vibrosuite software does use Microsoft SQL. Per default Microsoft SQL doesn’t install Java.

SQL Server (on Windows) – all editions

- Note: If a customer installs Java support and deploys Java Archives (JARs) that depend on the Log4j 2 library, they are advised to either upgrade to the latest version or remove the Java Archives (JARs) that require the dependency.

SETPOINT® Software

- Neither SETPOINT® CMS nor SETPOINT® CMS software uses any of the affected libraries. However, SETPOINT® CMS software does use OSIsoft® PI System® and OSIsoft® PI Vision™. Based on currently available information, OSIsoft® PI System® is unaffected by this vulnerability. Please refer to www.osisoft.com for more information.

In certain specific cases we use external components or software services to enable customized solutions. For these cases, we are reliant on the information available from the providers of these tools. As such we cannot rule out entirely that “log4j” might be embedded within such external components or software services.

Once any vulnerability has been discovered we will work closely with each vendor to evaluate the possible impact and determine the solutions that can be provided.

We will proactively reach out to any customers we believe to be affected.