Dear customers and users of our HMI system QuickHMI ,

probably you have already heard about the **Log4j security vulnerability** in the press:
With the help of a simple command, a critical vulnerability in the Java library Log4J allows arbitrary code to be executed on systems.
Log4j is one of the standard loggers in software developed with the Java programming language and is therefore very widely used. The "German Federal Office for Information Security" (BSI) issued the highest warning level for this already exploited zero-day vulnerability.

Unfortunately we have to inform you that our software QuickHMI is also affected by this vulnerability.
For this reason, we immediately took all steps recommended to close the gap and created a new version for our QuickHMI software suite. However, we are not currently aware of any specific cases.

Although we are not currently aware of any specific cases of misuse when using our software, **we strongly recommend that you use the latest official version (from version 9.4.2) of all software components (editor, runtime, viewer) and update older installations to the current version immediately.**

For questions and comments please contact our support team via email support@indi-an.de

QuickHMI Support-Team
Indi.An GmbH
Airport City
Flughafenallee 3
28199 Bremen
Germany
support@indi-an.de
Tel.:+49 421 989703-30
Fax:+49 421 989703-49
https://www.quickhmi.com/