IDS products not affected by Log4j vulnerability

Related to the recent disclosure of the vulnerability CVE-2021-44228, see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228, also known as "Log4j vulnerability", IDS Imaging Development Systems would like to inform our customers or other interested parties, that IDS products **are not affected** as follows.

All of IDS products including all of their components and versions, both self-developed by IDS or distributed exclusively by IDS, **are not affected** by the above mentioned vulnerability. Neither of our products make use of the mentioned Log4j library nor make use of any Java runtime components at all, i.e.

- **IDS peak** including the related uEye+ camera firmware
- **IDS Software Suite** including the related uEye camera firmware
- **IDS NXT** system tools like IDS NXT cockpit, IDS NXT ferry, etc. including the related camera firmware IDS NXT OS
- **IDS NXT lighthouse** web based deep learning training system
- **Ensenso SDK** including the related Ensenso camera firmware
- **Falcon & Eagle** drivers and the related frame-grabber firmware
- **IDS company websites and webstores**

For MVTec products like Halcon, Merlic, etc. distributed by IDS, please contact MVTec as the responsible manufacturer. According their public statement from Dec. 17th 2021 however, none of their products are affected.