Lund, 2022/01/10

Updated Statement from Axis Communications on the Log4j2 vulnerability (CVE 2021-44228)

On December 9th, researchers posted a proof of concept exploit titled Log4shell that demonstrates an exploit of a severe vulnerability in an Apache logging utility, Log4j2. Exploiting the vulnerability could allow an unauthenticated attacker to execute code remotely on the system running the utility.

Given the very public nature of this vulnerability and concern around the ease of exploitation, we would like to inform our partners and customers that we have completed our investigation into whether the Log4j2 utility is used in any of our hardware products, software or services. To the best of our knowledge, none of our systems appear to be affected by this vulnerability.

To clarify:

1. Hardware products running all versions of AXIS OS firmware including legacy products are **NOT** affected. More information can be found in the AXIS OS portal.
2. Hardware products not running AXIS OS such as Axis T85 switches, Axis NVRs and the AXIS Video Decoder are **NOT** affected.
3. Software products and their associated services including AXIS Camera Station, AXIS Companion, AXIS Device Manager 5, AXIS Device Manager Extend and AXIS Audio Manager Pro are **NOT** affected.
4. ACAP applications and any complementary configuration software developed by Axis and/or sold under the Axis name are **NOT** affected.

If there are further questions please contact Axis Technical Services.