Apache Log4J Vulnerability

Dear Customer,

You may be aware of the recently publicised critical Remote Control Execution (RCE) vulnerability in Apache Log4J.

We wanted to take this opportunity to reassure you that after reviewing our application for exposure to this vulnerability, we have determined that all our solutions (Libraesva ESG, Libraesva EA, Libraesva LB and Libraesva PhishBrain) are **not dependent** on the libraries containing the CVE-2021-44228 vulnerability (Log4Shell).

Further to this, we've verified that none of our public-facing cloud infrastructure is exposed to this vulnerability, with our penetration testers having completed a scan earlier this week.

We have also undertaken a full review of software packages used internally within Libraesva and are taking all appropriate actions to ensure that there is no potential exposure to this vulnerability.

Should you have any questions or concerns regarding any of the above, please contact support@libraesva.com where a member of the team will be happy to help.

Kind Regards,

The Libraesva Team