Hi <STUDENT\_NAME>,

Thank you for your insightful post and a well-presented sequence diagram.

Regarding vetting open-source software, companies typically have their *ad-hoc* processes in place, which are carried out following employees’ requests for approval of using a certain open-source library. Do you think this is true in your experience? If so, what would you suggest companies to adopt or do differently to be more proactive in identifying such vulnerabilities in open-source software? This is still particularly important considering recent large-scale vulnerabilities with Apache Log4j that had a global impact, including AWS customers (AWS, 2021).

I hope this helps.

Best regards,

Marianne

**Reference**

AWS (2021). AWS resources to address Apache Log4j vulnerabilities. Retrieved from https://aws.amazon.com/blogs/publicsector/aws-resources-to-address-apache-log4j-vulnerabilities/.