Syed Junaid Ahmed
Sp18-bcs-155
Assignment # 02

Question # 1

Answer: log4J is an open source project based on the work of many authors. It allows the developer to control which log statements are output with arbitrary granularity. It is fully configurable at runtime using external configuration files. Best of all, log4J has a gentle learning curve.

Question #2

Answer: Basically any device that exposed to the internet is at risk. If it's running Apache log4J, versions 2.0 to 2.14.1. NCSC notes that log4j version 2 (log4j2), the affected version, is included in Apache struts 2, Solr, Druid, flink and swift frameworks.

Question #3

Answer: Mitigation Measures

when updates are available, agencies must update software using log4j to the newest version, which is the most effective and managable long-term option. where updating is not possible, the following mitigating measures can be considerd as a temporary solution and apply to the entire solution stack.

- Disable log4j library.
- Disable JNDI lookups or disable remote codebases.
- Disconnect affected stacks.
- Isolate the system.
- Deploy a properly configured Web Application Firewall (WAF) in front of the solution stack.