Log4j Vulnerability – Update as of 30th December 2021, 15:30 GMT

On December 9, 2021, it was publicly reported, and Apache has confirmed, that a new, serious vulnerability was identified impacting Apache Log4j utility (CVE-2021-44228). On December 14 and 18, 2021, it was publicly reported, and Apache confirmed, that the fix to address CVE-2021-44228 was incomplete in certain non-default configurations. For additional details about this vulnerability, affected versions and solutions, please reference the Apache Logging Services alert.

Our priority is the security and integrity of our systems, data and customer data. At this time, there are no material impacts to our products or services.

We are aware of the additional threat intelligence relating to the Apache Log4j 2.15.0 and 2.16.0 fixes and have taken mitigating actions, including upgrading core Internet-facing applications to 2.17.0 or implementing mitigating controls (e.g., removal of the JNDI lookup class and JMS Appender).

Based on the threat intelligence and as the situation evolves, we will continue to monitor and assess the impact on Refinitiv systems.

For the three deployed applications listed in the table (i.e., applications installed on the customer sites), we recommend actioning per the notices below.

Refinitiv NEST Deployed	Refer to notice
Refinitiv Real-Time Advanced Transformation Server (ATS)	Refer to notice
FXall Quick Connect	Refer to notice

Please direct any questions you may have to the Helpdesk.