For Newgen on-premise and Cloud Customers

Update: 20th Dec'21 around Log4shell and Log4J upgrades

Newgen has released hotfixes for all Newgen Products as part of a two-prong approach for Log4J CVEs mitigation in Newgen Solutions

1) Newgen Product Hotfix upgrade for vulnerable Log4J 2.x to the latest version of Log4J 2.17 for Java 8 (or later) and Log4J 2.12.2 for Java 7.
2) Interim Newgen Product hotfixes for lower versions of Log4J 1.x (*not vulnerable for Log4Shell*) addressing the older CVEs (*CVE-2019-17571 and CVE-2021-4104*).

Meanwhile, for the customization over Product, until the time upgrade to the latest option is not available; if the application is not using the log4j-core JAR, you may delete the JAR, otherwise, the JndiLookup class is not available from the log4j-core jar may be removed (*refer Apache Log4j Security update*).

Newgen is closely monitoring the Log4j CVEs new developments and will take all possible measures for protecting Our Customer Deployments. You may coordinate with Newgen Engagement manager/Project Team for further assistance around released hotfixes.

InfoSec Team

Newgen Software

newgen.infosec@newgensoft.com

Communication ID: SEC/PROD/20122021/01