For Newgen on-premise Customers

Update: 13th Dec'21 around Log4shell

Newgen is aware of the recently disclosed security issue relating to the open-source Apache "Log4j2" utility (CVE-2021-44228). Newgen products are not using Log4j vulnerable version and thus is not affected by Log4Shell issue (CVE-2021-44228).

However, some of the customization over Product are using Log4j vulnerable version. We are closely monitoring this issue while continuously updating our controls/definitions.

Meanwhile, the following may be implemented as a precautionary measure in your environments

1. Restrict all Egress towards internet, and if required, only allow through whitelisting [Basic hardening practice]
2. Till the time a permanent fix for the customization over Product is not released, we recommend to apply any of the below options, whichever applicable
    a. Log4J 2 versions 2.10 to 2.14.1 support the parameter log4j2.formatMsgNoLookups to be set to 'true', to disable the vulnerable feature. Ensure this parameter is configured in the startup scripts of the Java Virtual Machine:
        -Dlog4j2.formatMsgNoLookups=true
    b. Alternatively, customers using Log4j 2.10 to 2.14.1 may set the LOG4J_FORMAT_MSG_NO_LOOKUPS=" true" environment variable to force this change.
    c. If the server has Java runtimes later than 8u121, then it is protected against remote code execution by defaulting "com.sun.jndi.rmi.object.trustURLCodebase" and "com.sun.jndi.cosnaming.object.trustURLCodebase" to "false"

You may coordinate with Newgen Engagement manager/Project Team for further assistance.

InfoSec Team

Newgen Software

newgen.infosec@newgensoft.com

Communication ID: SEC/PROD/13122021/01