Knowledge Base Article #PG5842, Rev C

PolicyGuru® Meta-Policy Controller 2.6.x: Mitigation for Apache Log4j CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832

Synopsis

This document provides procedures to mitigate CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832 for log4j components within the PolicyGuru® v2.6.x system. Certain PolicyGuru System components must be stopped to update the underlying log4j components, but you do not need to stop the **ngp** service to apply this patch.

Note: No changes are required on the Database or ENUM Servers.

Versions Affected

PolicyGuru® v2.6.x

Mitigation Procedures for PolicyGuru® v2.6.x

Before you begin, obtain the following files from SecureLogix Technical Support:

- **log4j-core-2.17.1.jar**
- **log4j-api-2.17.1.jar**

Mediation Server Procedure

Perform the following steps on the Mediation Server. (You do not need to stop the **ngp** service.) It is recommended that you save copies of the original files that are being replaced into a folder outside of the **/opt/ngp** directory structure.

To update the Mediation Server

1. Download the **amazon-corretto-8.312.07.1-linux-x64.tar.gz** file (containing the Amazon Corretto 8 JDK) using this link: https://corretto.aws/downloads/latest/amazon-corretto-8-x64-linux-jdk.tar.gz. Untar this file on the system in the desired folder. For instance, this file could be copied to the **/opt** folder (or other preferred location) and untarred using the command **tar xzvf amazon-corretto-8.312.07.1-linux-x64.tar.gz**. The Corretto 8 JDK will be used for running the updated SLC EIP tools (see below).
2. Stop any of the tools that use the SLC EIP package, including CAS Agent, PG-Stream Transceiver, and ProbeSIPFlow Archiving Transceiver.
   - To stop the CAS Agent, use the following command:

     ```
     /opt/ngp/bin/pmf_util.sh stop CASAgentProcessMonitor
     ```
   - The PG-Stream Transceiver and ProbeSIPFlow Archiving Transceiver are typically stopped by finding their running Process ID (PID), and then issuing the `kill <PID>` command..
3. Replace **/opt/slc/slc-eip/lib/log4j-core-2.8.2.jar** with the provided **log4j-core-2.17.1.jar** file.

4. Replace **/opt/slc/slc-eip/lib/log4j-api-2.8.2.jar** with the provided **log4j-api-2.17.1.jar** file.
5. Edit the **/opt/ngp/pg-cas-agent/run.sh** file and preface the Java command with the path to the new Amazon Corretto 8 Java executable. For instance, if the new JDK was untarred in **/opt**, the Java command in **run.sh** would be **"/opt/amazon-corretto-8.312.07.1-linux-x64/bin/java"**.
6. If the PG-Stream Transceiver is installed, edit the **/opt/ngp/pg-stream/run.sh** file and preface the Java command with the path to the new Amazon Corretto 8 Java executable. For instance, if the new JDK was untarred in **/opt**, the Java command in **run.sh** would be **"/opt/amazon-corretto-8.312.07.1-linux-x64/bin/java"**.
7. If the ProbeSIPFlow Archiving Transceiver is installed, edit the **/opt/ngp/probesipflow-archiving-transceiver/run.sh** file and preface the Java command with the path to the new Amazon Corretto 8 Java executable. For instance, if the new JDK was untarred in **/opt**, the Java command in **run.sh** would be **"/opt/amazon-corretto-8.312.07.1-linux-x64/bin/java"**.
8. After replacing/editing the above files, restart the CAS Agent and ProbeSIPFlow Archiving Transceiver, if they were running previously.

   - To start the CAS Agent, use the following command:

     ```
     /opt/ngp/bin/pmf_util.sh start CASAgentProcessMonitor
     ```

   - The PG-Stream Transceiver can be manually restarted by changing to the **/opt/ngp/pg-stream/** directory and issuing the command:

     ```
     nohup ./run.sh &>/dev/null &
     ```

   - The ProbeSIPFlow Archiving Transceiver ca be manually restarted by changing to the **/opt/ngp/probesipflow-archiving-transceiver/** directory and issuing the command:

     ```
     nohup ./run.sh &>/dev/null &
     ```

Metadata Probe Server Procedure

Perform the following steps to update log4j on Metadata Probe Servers that are using the ProbeSIPFlow Archiving Transceiver. (You do not need to stop the **ngp** service.) It is recommend that you save copies of the original files that are being replaced into a folder outside of the **/opt/ngp** directory structure.

To update the Probe Server

1. On Probe servers, check whether the ProbeSIPFlow Archiving Transceiver and the associated **slc-eip** RPM are installed. If they are installed, perform the following steps.
2. Download the **amazon-corretto-8.312.07.1-linux-x64.tar.gz** file (containing the Amazon Corretto 8 JDK) using this link: https://corretto.aws/downloads/latest/amazon-corretto-8-x64-linux-jdk.tar.gz. Untar this file on the system in the desired folder. For instance, this file could be copied to the **/opt** folder (or other preferred location) and untarred using the command **tar xzvf amazon-corretto-8.312.07.1-linux-x64.tar.gz**. The Corretto 8 JDK will be used for running the updated ProbeSIPFlow Archiving Transceiver.
3. Replace **/opt/slc/slc-eip/lib/log4j-core-2.8.2.jar** with the provided **log4j-core-2.17.1.jar** file.

4. Replace **/opt/slc/slc-eip/lib/log4j-api-2.8.2.jar** with the provided **log4j-api-2.17.1.jar** file.

5. Edit the **/opt/ngp/probesipflow-archiving-transceiver/run.sh** file and preface the java command with the path to the new Amazon Corretto 8 Java executable. For instance, if the new JDK was untarred in **/opt**, the Java command in **run.sh** would be **"/opt/amazon-corretto-8.312.07.1-linux-x64/bin/java"**.

6. After replacing/editing the above files, restart the ProbeSIPFlow Archiving Transceiver if it was running previously. The ProbeSIPFlow Archiving Transceiver can be manually restarted by changing to the **/opt/ngp/probesipflow-archiving-transceiver/** directory and issuing the command:

   ```
   nohup ./run.sh &>/dev/null &
   ```

Last Update: 1/21/2022

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232
(210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • support.securelogix.com