PowerChute Business Edition Log4JShell Mitigation Scripts

Windows

Overview

The file *mitigate_log4shell.cmd* will execute a powershell script called *PCBE_mitigate_Log4shell.ps1* to mitigate CVE-2021-44228 and CVE-2021-45046 per the guidance in https://logging.apache.org/log4j/2.x/security.html. It does this by stopping the PowerChute Business Edition Agent service, deleting the JndiLookup class from the classpath and then re-starting the service.

Prerequisites

PowerShell version 3.0 or later installed on your system.

.NET Framework version 4.5.0 or later installed on your system.

Note: If the above are not available or cannot be installed please refer to the manual steps in this security bulletin.

The powershell script will not run unless the above are installed.

How to run the script

Copy *PCBE_Scripts.zip* file to the machine where PowerChute is installed and extract the contents to a folder on that machine.

Open a windows command prompt as administrator (In the Windows Start Menu, search for 'Command Prompt', right-click the 'Command Prompt' application, and select 'Run as administrator' from the context menu). The scripts must be run as an administrator to have the necessary permissions to interact with the service and write to the log4jcore* jar file on the file system.

Change directory to the location where you extracted the files, type mitigate_log4shell.cmd and press return to execute the PCBE_mitigate_Log4shell.ps1 file.

After running the script, org/apache/logging/log4j/core/lookup/JndiLookup.class will have been removed from log4j-core, mitigating the risk.

Linux

Overview

The shell script called *PCBE_Mitigate_Log4Shell.sh* will mitigate CVE-2021-44228 and CVE-2021-45046 per the guidance in https://logging.apache.org/log4j/2.x/security.html. It does this by stopping the PowerChute service, deleting the JndiLookup class from the classpath and then re-starting the service.

Prerequisites

The zip and sed libraries must be installed on the target system. These can be installed using a package manager such as yum, zypper or apt-get depending on your Linux Operating System e.g. for RedHat Linux run:

1. yum install unzip
2. yum install zip

How to run the script

Copy PCBE_Scripts.zip file to the machine where PowerChute is installed and extract the contents to a folder on that machine.

Open a terminal prompt or connect to the target machine via SSH.

Change directory to the folder where the files were extracted and move to the Linux folder.

As root user or use sudo:

- Type chmod +x ./PCBE_Mitigate_Log4Shell.sh
- Type ./PCBE_Mitigate_Log4Shell.sh and press return
- The script will attempt to locate the PowerChute installation directory. When prompted press Enter to select this directory, or alternatively you can manually enter the path to the installation directory (the directory containing the 'lib' folder).
- Confirm that you are happy to proceed with running the script.

After running the script, org/apache/logging/log4j/core/lookup/JndiLookup.class will have been removed from log4j-core, mitigating the risk.