How To: Run the Log4Shell Mitigation Script for ArcGIS Workflow Manager Server

Summary

The Log4Shell vulnerability (CVE-2021-44228) is a critical security vulnerability in version 2 of the log4j library. ArcGIS Workflow Manager Server does use an impacted version 2 of log4j at version 10.9.1 only, earlier versions of Workflow Manager Server do not use log4j and are therefore unaffected by this vulnerability. This article provides steps to mitigate the risk of exploitation. Esri is working towards a patch, but this mitigation script can be used immediately on ArcGIS Workflow Manager Server version 10.9.1.

How This Script Works:
This script implements a widely documented industry approach of modifying version 2 log4j libraries to remove the JndiLookup.class file from the "core" log4j jar file so that the vulnerability can't be exploited. This script identifies all locations in ArcGIS Workflow Manager Server where the class files reside and then removes those class files. The script has two implementations – one for Linux and one for Windows. These same scripts can be used against ArcGIS Server, ArcGIS Data Store, and Portal for ArcGIS, so if you have downloaded the log4shellmitigation script for those products then you can re-use it for these steps.

Prerequisites:

- Windows - the script requires Python3 to be installed, Python 2.7 will not work. You can use the Python3 that comes with ArcGIS Server installed on the same ArcGIS Workflow Manager Server machine. You can find Python 3 installed on your machine in the following location:
    - ArcGIS Server: Python 3 is typically installed in your ArcGIS Server directory (commonly C:\Program Files\ArcGIS\server in Windows) under the \framework\runtime\ArcGIS\bin\Python\envs\arcgispro-py3 directory.
- Linux – the script requires the bash shell and the zip command to be installed. Most likely bash is already installed, and it will be unnecessary to install it. Depending on the Linux distribution and version being used, you may need to install the zip program using either apt-get or yum.

To verify the version of Python you are running, open a command prompt and type the following:

```
<full path to Python>\python.exe –version
```

Note:
Esri recommends verifying that you have the correct download before running these scripts. To do so, run checksum on the downloaded zip files and verify that the hash is identical to that shown in the table below. For more information about running checksum, see the following article: How To: Verify an Esri download using the checksum

If the file hash does not match with what is shown below, clear your browser cache and download the file again.

Operating system	File name	Hash
Windows	log4shellmitigation.python.zip	31EC8F0543348498000B7B36E0ED17354EAAE14C3B131ACC3877B6E1918D58F3
Linux	log4shellmitigation.linux.zip	DDB01B31CF7B91270DF4410F502B17D42DC21232661400982D500E79C577897B

Procedure

Windows Workflow

The following steps work for ArcGIS Workflow Manager Server version 10.9.1

Preparation

1. Login as administrator or the ArcGIS Workflow Manager Server "run as" account. This account must have permissions to modify files in the ArcGIS Workflow Manager Server directory.

2. Download the log4shellmitigation.python.zip file to the ArcGIS Workflow Manager Server machine and unzip it. It can be placed in any location.
3. Start a command prompt.
4. Change directories ("cd") into directory where you placed the script.
5. Enter the following command:

```
<full path to Python>\python.exe log4shellmitigation.py --list <ArcGIS Server install directory>
```

Here's an example of the command:

```
"C:\Program Files\ArcGIS\Server\framework\runtime\ArcGIS\bin\Python\envs\arcgispro-py3\python.exe" log4shellmitigation.py -l
"C:\Program Files\ArcGIS\Server"
```

This lists all the files that will be changed. Make note of these locations in case you want to revert the changes later.

Note:
The ArcGIS Server install directory is commonly "C:\Program Files\ArcGIS\Server". If the path to Python or the ArcGIS Server installation has spaces in it, please put quote marks (") around the path.

Note that the command flag is -l (dash lowercase ell), missing a dash or inserting a space will cause the command to fail.

Executing the script

6. Stop the ArcGIS Server and ArcGIS Workflow Manager Server services, the command used in the following steps won't be able to modify the files if these ArcGIS Windows Services are running.
7. Now enter the following command:

```
<full path to Python>\python.exe log4shellmitigation.py --delete <server directory>
```

Here's an example of the command:

```
"C:\Program Files\ArcGIS\Server\framework\runtime\ArcGIS\bin\Python\envs\arcgispro-py3\python.exe"  log4shellmitigation.py --
delete "c:\Program Files\ArcGIS\Server"
```

This is the command that is modifying the JAR files so that log4shell cannot be exploited.

8. Start the ArcGIS Server service.
9. Start the ArcGIS Workflow Manager service.

Troubleshooting

If there are any problems and it is necessary to roll back the changes, please contact Esri Technical Support for assistance.

Linux Workflow

Preparation

The following steps work for ArcGIS Workflow Manager Server version 10.9.1.

1. Log into your Linux machine running ArcGIS Workflow Manager Server with the account that installed ArcGIS Workflow Manager Server. Do not use a different non-root account, root account or superuser.
2. Download the log4shellmitigation.linux.zip file to the ArcGIS Workflow Manager Server machine and unzip it. It must be placed into the parent directory of your ArcGIS Server location.

For example, if ArcGIS Server was installed in /opt/arcgis/server then you would need to place the script in the /opt/arcgis directory.

Note:
If you have multiple ArcGIS Enterprise products installed on the same machine with the same parent directory and you have already run the log4shellmitigation.sh script from that same location, it is not necessary to run again. Running the script from a parent directory will apply it to all products that share the same parent directory.

3. Change directory into the parent directory where you placed the log4shellmitigation.sh script.
4. Make the script executable using this command:

```
chmod 500 log4shellmitigation.sh
```

5. Run the script using the -l (dash el) option to identify all the files that will be changed.

```
./log4shellmitigation.sh -l
```

This lists all the files that will be modified. No backup of these files will be made by this script. If you wish to back up these original files, do so now by copying them to some other location.

6. Stop ArcGIS Server and Workflow Manager Server. You can use any means you normally use.
7. Run the script with no arguments:

```
./log4shellmitigation.sh
```

8. When prompted, confirm that you wish to proceed with patching the files by entering 'y'.
9. Start ArcGIS Server and Workflow Manager Server. You can use any means you normally use.

Troubleshooting

If there are any problems and you wish to roll back the changes, please contact Esri Technical Support for assistance.

Related Information

- How To: Run the Log4Shell Mitigation Script for ArcGIS Server
- How To: Run the Log4Shell Mitigation Script for Portal for ArcGIS
- How To: Run the Log4Shell Mitigation Script for ArcGIS Data Store
- How To: Run the Log4Shell Mitigation Script for ArcGIS GeoEvent Server
- How To: Run the Log4Shell Mitigation Script for ArcGIS GeoEnrichment Server
- How To: Verify an Esri download using the checksum
- Problem: Unable to execute a python file in Windows Command Prompt

Last Published: 12/21/2021

Article ID: 000026970