How To: Run the Log4Shell Mitigation Script for GeoEnrichment Server

Summary

The Log4Shell vulnerability (CVE-2021-44228) is a critical security vulnerability in version 2 of the log4j library. 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 all versions of GeoEnrichment Server.

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 GeoEnrichment 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, Portal for ArcGIS, and ArcGIS Data Store and 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 download any recent release of Python3 to run the script. Afterwards you can remove Python3.
- **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.

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

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

Procedure

Windows Workflow:
The following steps work for any version of GeoEnrichment Server.

Preparation

1. Login as administrator or the GeoEnrichment "run as" account. This account must have permissions to modify files in the GeoEnrichment directory.
2. Download the log4shellmitigation.python.zip file and unzip it to the GeoEnrichment machine. 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 <geoenrichment directory>

Here's an example of the command:

```
C:\Users\YourUserName\AppData\Local\Programs\Python\Python310\python.exe log4shellmitigation.py --list "c:\Program Files\ArcGIS\GeoEnrichment"
```

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

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

Note that it is "dash dash list" --list. Missing a dash or inserting a space will cause the command to fail.

6. This script may take a minute to run as it looks through every file in the GeoEnrichment directory. This lists which files will be updated when you run the script in 'delete' mode. Take note of these in case you need to revert the changes.

Executing the script

7. Stop the GeoEnrichment Data Store service. The following command won't be able to modify the files if GeoEnrichment Server is running.
8. Enter the following command:

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

Here's an example of the command:

```
C:\Users\YourUserName\AppData\Local\Programs\Python\Python310\python.exe log4shellmitigation.py --delete "c:\Program Files\ArcGIS\GeoEnrichment"
```

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

9. Start the GeoEnrichment Data Store service.

Troubleshooting

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

Linux Workflow

The following steps should work against any version of GeoEnrichment Server.

Preparation

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

For example, if GeoEnrichment Server were installed in /opt/arcgis/geoenrichment then you must 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 GeoEnrichment Server. You can use any means you normally use but running the stopdatastore.sh script in the <GeoEnrichment Installation Location>/arcgis/geoenrichment directory will work across most versions of Linux distributions.
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 the GeoEnrichment service. You can use any means you normally use, but running the startdatastore.sh script in the <GeoEnrichment Installation Location>/arcgis/geoenrichment directory will work across most versions of Linux distributions.

Troubleshooting

If there are any problems and it is necessary 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 Workflow Manager 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: 000026982