

Esri Support app 4.1 available

News >

Download now!



Esri Support app 4.1 available 1

Download now!



Take advantage of our 8 new features

About >

Learn more.

How To: Run the Log4Shell Mitigation Script for Portal for ArcGIS

Summary

The Log4Shell vulnerability (CVE-2021-44228) is a critical security vulnerability in version 2 of the log4j library. Although Portal for ArcGIS doesn't directly use version 2 of log4j, one of the included libraries, elasticsearch for the implementation of the index service, does use version 2 of log4j. 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 the Portal for ArcGIS versions 10.6 and above. The script may work on versions before 10.6, but it is untested on those versions.

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 Portal for ArcGIS 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 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. Python is installed in your Portal installation directory (commonly C:\Program Files\ArcGIS\Portal) under the \framework\runtime\python 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.

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	71C96FB3D31C0EC6F776D590A7763080B79E917BD2C5EB799C7121B3E3197041

Procedure

Windows Workflow

The following steps work for any version of Portal for ArcGIS 10.6 and higher.

Preparation

1. Login as administrator or the Portal for ArcGIS "run as" account. This account must have permissions to modify files in the Portal for ArcGIS directory.
2. Download the [log4shellmitigation.python.zip](#) script to the Portal for ArcGIS machine and unzip it. The .py script contained 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 <portal directory>
```

Here's an example of the command:

```
"c:\Program Files\ArcGIS\Portal\framework\runtime\python\python.exe" log4shellmitigation.py --list "C:\Program Files\ArcGIS\Portal"
```

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 portal directory is commonly "C:\Program Files\ArcGIS\Portal"

If the path to Python or the Portal 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.

This script may take a minute to run as it looks through every file in the Portal for ArcGIS 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

6. Stop the Portal for ArcGIS service. The following command won't be able to modify the files if Portal for ArcGIS is running.

7. Enter the following command:

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

Here's an example of the command:

```
"c:\Program Files\ArcGIS\Portal\framework\runtime\python\python.exe" log4shellmitigation.py --delete "C:\Program Files\ArcGIS\Portal"
```

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

8. One other location also must be updated with Portal for ArcGIS. Enter the following command:

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

Here's an example of the command:

```
"c:\Program Files\ArcGIS\Portal\framework\runtime\python\python.exe" log4shellmitigation.py --delete "C:\arcgisportal"
```

9. Start the Portal for ArcGIS 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 should work against any version of Portal for ArcGIS 10.6 and higher.

1. Log into your Linux machine running Portal for ArcGIS with the account that installed Portal for ArcGIS. Do not use a different non-root account, root account or superuser.
2. Download the [log4shellmitigation.linux.zip](#) to the Portal for ArcGIS machine and unzip it. The .sh script must be placed into the parent directory of your Portal for ArcGIS location.

For example, if Portal for ArcGIS were installed in /opt/arcgis/portal 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 to 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 ell) 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 Portal for ArcGIS. You can use any means you normally use, but running the stopportal.sh script in the <Portal Installation Location>/arcgis/portal 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 Portal for ArcGIS. You can use any means you normally use, but running the startportal.sh script in the /arcgis/portal 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 Data Store](#)
- [How To: Run the Log4Shell Mitigation Script for ArcGIS Server](#)
- [How To: Run the Log4Shell Mitigation Script for ArcGIS GeoEvent Server](#)
- [How To: Verify an Esri download using the checksum](#)

Last Published: 12/15/2021

Article ID: 000026950

Software: Portal for ArcGIS 10.9.1, 10.9, 10.8.1, 10.8, 10.7.1, 10.7, 10.6.1, 10.6



ARCGIS

COMMUNITY

UNDERSTANDING GIS

COMPANY

SPECIAL PROGRAMS

Switch Language

[Privacy](#) [Trust Center](#) [Legal](#) [Site Map](#) [Code of Business Conduct](#)