How To: Run the Log4Shell Mitigation Script for ArcGIS GeoEvent Server

Summary

The Log4Shell vulnerability (CVE-2021-44228) is a critical security vulnerability in version 2 of the log4j library. ArcGIS GeoEvent Server does use an impacted 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 ArcGIS GeoEvent Server 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 files so that the vulnerability can't be exploited. This script identifies all locations in the ArcGIS GeoEvent 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 GeoEvent 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 any version of ArcGIS GeoEvent Server 10.6 and higher.

Preparation

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

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

```
<full path to Python>\python.exe log4shellmitigation.py -l <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 el), 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 ArcGIS Server and ArcGIS GeoEvent Server directories. This will list 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 all the Windows Services related to ArcGIS, the command used in the following steps won't be able to modify the files if the ArcGIS Windows Services are running:
    - ArcGISGeoEvent
    - ArcGISGeoEventGateway
    - ArcGIS Server
    - ArcGIS Data Store
    - Portal for ArcGIS
7. In File Explorer, navigate to the GeoEvent installation directory and delete the contents of the /data/ directory (do not delete the /data/ directory itself).

Example location:

```
"C:\Program Files\ArcGIS\Server\GeoEvent\data\"
```

8. Enter the following command:

```
<full path to Python>\python.exe log4shellmitigation.py -d <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 -d
"C:\Program Files\ArcGIS\Server"
```

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

9. Start ArcGIS Windows Services *in the following order*:
    a. Portal for ArcGIS
    b. ArcGIS Server
    c. ArcGIS Data Store
    d. ArcGISGeoEventGateway
    e. ArcGISGeoEvent

Note that it may take a minute or two for GeoEvent Server to start up.

Troubleshooting

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

Linux Workflow

Preparation

The following steps should work against any version of ArcGIS GeoEvent Server 10.6 and higher.

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

For example, if ArcGIS Server was installed in /home/arcgis/server then you would need to place it in the /home/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 all running ArcGIS services. You can use any means you normally use.
7. Delete the contents of the /data/ directory under the GeoEvent Server installation (do not delete the /data/ directory itself).

Example location:

```
"/home/arcgis/server/GeoEvent/data"
```

8. Run the script with no arguments:

```
./log4shellmitigation.sh
```

9. When prompted, confirm that you wish to proceed with patching the files by entering 'y'.
10. Start the ArcGIS services *in the following order*. You can use any means you normally use to start the services
    a. Portal for ArcGIS
    b. ArcGIS Server
    c. ArcGIS Data Store
    d. ArcGISGeoEventGateway
    e. ArcGISGeoEvent

Rollback

If there is a need to revert the changes made by the script, you must stop the ArcGIS services, copy back the files you backed up, and then restart the ArcGIS services, making sure to restart them in the order listed in step 10 above.

Related Information

- 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 Server
- How To: Verify an Esri download using the checksum

Last Published: 12/16/2021

Article ID: 000026956