Security Advisory 2021-073

# Adobe ColdFusion Critical Vulnerability

*December 17, 2021 — v1.0*

**TLP:WHITE**

*History:*

- *17/12/2021 — v1.0 – Initial publication*

## Summary

On December 16th, Adobe updated its security advisory related to CVE-2021-44228 affecting ColdFusion products [1]. While this CVE affects the Java logging library log4j, all products using this library are vulnerable to Unauthenticated Remote Code Execution [2].

## Technical Details

The vulnerability exists in the Java logging library log4j. An unauthenticated remote attacker might exploit this vulnerability by sending specially crafted content to the application to execute malicious code on the server [2].

## Affected products

- ColdFusion 2021 release - contains the vulnerable Log4j versions 2.13.3
- ColdFusion 2018 release - contains the vulnerable Log4j versions 2.13.3 and/or 2.9.0
- Performance Monitoring Toolset 2021 - contains the vulnerable Log4j versions 2.11.1 and 2.3
- Performance Monitoring Toolset 2018 - contains the vulnerable Log4j versions 2.9.1 and 2.3
- API Manager 2021, 2018, and 2016 - contains the vulnerable Log4j versions 2.3

## Workaround and mitigation

Adobe plans to release a patch for the log4j vulnerability to ColdFusion's customers the 17/12/2021. In the meantime, they recommend to apply these mitigation steps until the patch is released.

The mitigation steps, according to the product and the version are presented below:

### ColdFusion 2021

- Stop the server.
- Navigate to the directory `<cf_root>\<Instance_name>\bin`.

- Open `jvm.config` file and add `-Dlog4j2.formatMsgNoLookups=true` argument in `java.args` section. Save the file.
- If using any third-party libraries that use Log4j2, and hence vulnerable, search for log4j-core in `<cf_root>` directory. If the Log4j2 version (<= 2.10 and >=2.0-beta9) is found, remove the `JndiLookup` class from the classpath like below, otherwise skip this step.
  - If the Operating System is Windows , then unzip the `log4j-core-2.x.jar` file and remove the class from path: `org/apache/logging/log4j/core/lookup/JndiLookup.class` and zip the `log4j-core-2.x.jar`. `X` is the version number you found in the folder.
  - If the Operating System is non-windows, then remove the `JndiLookup` class from the classpath : `zip -q -d log4j-core-2.x.jar  org/apache/logging/log4j/core/lookup/JndiLookup.class`. `X` is the version number you found in the folder.
- Restart the instance.
- Repeat the procedure for all other instances.

### ColdFusion 2018

- Stop the server.
- Navigate to the directory `<cf_root>\<Instance_name>\bin`.
- Open `jvm.config` file and add `-Dlog4j2.formatMsgNoLookups=true` argument in `java.args` section. Save the file.
- If you find the file `log4j-core-2.9.0.jar`, move the file to a temporary location.
- Copy the patched `log4j-core-2.9.0.jar` file with `JNDILookUp` class that you have removed. The new file can be downloaded on Adobe website [3].
- If you are using any third-party libraries that use log4j2, and hence vulnerable, search for log4j-core in `<cf_root>` directory. If log4j2 version (<= 2.10 and >=2.0-beta9) is found, remove the `JndiLookup` class from the classpath as mentioned below, otherwise skip this step:
  - If the Operating System is Windows, then unzip the `log4j-core-2.x.jar` file and remove the class from path : `org/apache/logging/log4j/core/lookup/JndiLookup.class` and zip the log4j-core-2.x.jar. `X` is the version number that you found in the folder.
  - If the Operating Systems is non-Windows, then remove the `JndiLookup` class from the classpath : `zip -q -d log4j-core-2.x.jar  org/apache/logging/log4j/core/lookup/JndiLookup.class`. `X` is the version number that you found in the folder.
- Restart the instance and delete `log4j-core-2.9.0.jar` from the temporary location.
- Repeat the procedure for all other instances.

### Performance Monitoring Toolset 2021

- Stop the Performance Monitoring Toolset and datastore services.
- Navigate to the directory `<PMT_Home>\datastore\config`.
- Open the file `jvm.options`, add `-Dlog4j2.formatMsgNoLookups=true` argument in `#log4j2` section. Save the file.
- Navigate to the directory `<PMT_Home>\lib`.
- Move the file `log4j-core-2.3.jar` to a temporary location.
- Copy the patched `log4j-core-2.3.jar` file with `JNDILookUp` class removed. The file can be downloaded from Adobe website [4].
- Restart the Performance Monitoring Toolset and datastore services.
- Delete `log4j-core-2.3.jar` from the temporary location.

### Performance Monitoring Toolset 2018

- Stop the Performance Monitoring Toolset and datastore services.
- Navigate to the directory `<PMT_Home>\datastore\lib`.
- Move the file `log4j-core-2.9.1.jar` to a temporary location.
- Copy the patched `log4j-core-2.9.1.jar` file with `JNDILookUp` class removed. The file can be downloaded from Adobe website [5].
- Navigate to the directory `<PMT_Home>\lib`.
- Copy the file `log4j-core-2.3.jar` to a temporary location.
- Copy the patched `log4j-core-2.3.jar` file with `JNDILookUp` class removed. The file can be downloaded from Adobe website [4].
- Restart the Performance Monitoring Toolset and datastore services.
- Delete `log4j-core-2.3.jar` and `log4j-core-2.9.1.jar` from the temporary location.

### API Manager 2021, 2018, and 2016

- Stop the API Manager server ( `<APIM_Home>\bin` ) and Analytics ( `<APIM_Home>database\analytics\bin` ) service.
- Navigate to the directory `<APIM_Home>\lib`.
- Move the file `log4j-core-2.3.jar` to a temporary location.
- Copy the patched `log4j-core-2.3.jar` file with `JNDILookUp` class removed. The file can be downloaded from Adobe website [4].
- Restart the Analytics service and the API Manager server.
- You can now delete `log4j-core-2.3.jar` from the temporary location.

## References

[1] https://helpx.adobe.com/ch_fr/coldfusion/kb/log4j-vulnerability-coldfusion.html

[2] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf

[3] https://cfdownload.adobe.com/pub/adobe/coldfusion/logshell/2.9.0/log4j-core-2.9.0-logshell.jar

[4] https://cfdownload.adobe.com/pub/adobe/coldfusion/logshell/2.3/log4j-core-2.3-logshell.jar

[5] https://cfdownload.adobe.com/pub/adobe/coldfusion/logshell/2.9.1/log4j-core-2.9.1-logshell.jar