


# Log4j impacts on Data Movement products

Last updated by | Krishnakumar Rukmangathan | Jan 14, 2022 at 12:20 AM PST

## Contents


- [ISSUE](#)
- [Current Status](#)
  - [Managed IR \(Azure IR, Azure-SSIS IR and Managed VNet IR\)](#)
  - [On-premise products: SHIR and SQL Server Integration Ser...](#)
  - [Data flow: The log4j library used in Dataflow Databricks alr...](#)
- [Mitigation Steps of Manually Upgrade log4j from 1.x to 2.x:](#)
- [Patch ETA](#)
- [Public doc](#)
- [More detail below](#)
  - [SHIR:](#)
  - [Dataflow](#)
  - [SSIS](#)
  - [Azure Purview](#)
- [Reference:](#)

## ISSUE

The open source component Apache Log4J versions 2.0 through 2.14.1, inclusive contains a critical security vulnerability CVE-2021-44228. More details can be found here: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228> 

## Current Status

The Data Factory components SSIS, SHIR, Data Flow will leverage library Log4j (1.X), Microsoft's Response to CVE-2021-44228 Apache Log4j 2 – Microsoft Security Response Center is only for 2.X, so the ADF is not related to the security hole known issue.

Regarding 1.X again, we have customer mentioned that CVE - CVE-2019-17571 ([mitre.org](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17571) ) might be the vulnerability issue, however, the ORC and parquet will leverage the JVM just for format serialization/deserialization, so this CVE has no impact on Data Factory.




Note: This applies to below ADF products:

**Managed IR (Azure IR, Azure-SSIS IR and Managed VNet IR)**

**On-premise products: SHIR and SQL Server Integration Services (SSIS).**

**Data flow: The log4j library used in Dataflow Databricks already contains the fix for it.**

## Mitigation Steps of Manually Upgrade log4j from 1.x to 2.x:

1. Remove these 2 .jar packs from "Jars" folder of SHIR (C:\Program Files\Microsoft Integration Runtime\5.0\Gateway\Jars)
2. Download those .jar packs from: a. log4j-1.2-api-2.17.0.jar:  
<https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-1.2-api/2.17.0>  b. log4j-api-2.17.0.jar:  
<https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-api/2.17.0>  c. log4j-core-2.17.0.jar:  
<https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core/2.17.0> 
3. Copy those 3 .jar packs into "Jars" folder of SHIR.
4. Done. It takes effect immediately. You don't need to restart SHIR. I also zipped the 3 .jar packs and put it in this temp storage. You may get it from here if you don't want to download them from Maven.

## Patch ETA

Mid Jan 2022

## Public doc

[Troubleshoot security and access control issues - Azure Data Factory & Azure Synapse | Microsoft Docs](#) 

## More detail below

### SHIR:

[Incident-277437591 Details - IcM](#) 

ORC/Parquet format (Open source) in SHIR references log4j-1.2.17.jar. As Log4j 1.x has reached end of life and is no longer supported, which breaks vulnerabilities check, we definitively will release a new SHIR with patch to update the version. But PG team needs buffer to fully test the new version and evaluate the impact/any breaking changes so we cannot provide the ETA right now. As work around, if customer doesn't use ORC, parquet format in their copy activity, he can go to this file path C:\Program Files\Microsoft Integration Runtime\5.0\Gateway\Jars and remove the log4j-1.2.17.jar file directly.

### Dataflow

[Incident-277290016 Details - IcM](#) 

Summary : Log4j2 library is only used in test environment. For the data flow impact of "CVE-2019-17571" (the old vulnerability issue), the log4j library used in Databricks already contains the fix for it.

Unfortunately, the log4j library version of data flow is controlled by spark execution environment (i.e. Databricks, Synapse Spark) instead of our runtime repo, so we can't easily upgrade the version by ourselves. Currently there's no ETA for working with our partner team to get the latest log4j installed.

## SSIS

For On-Prem SSIS - Refer to the [Email Template for Customer Communication](#) 

[Hotfix 14482693:Hotfix for log4j2 Vulnerability to SQL Server SSIS](#) 

[RFC 14428766: log4j2 Vulnerability to SQL Server SSIS - Microsoft Team Foundation Server](#) 

We have log4j file under Microsoft SQL Server\Program Files\Microsoft SQL Server\150\DTS\Extensions\Common\Jars. PG replied in email confirming that the version of log4j (1.x) in SSIS is not vulnerable, only version 2.x is vulnerable.


#### FAQs:


1. Can we manually remove/delete Log4j (1.X) JAR files from SQL Server 2019 installation path (i.e. Program Files\Microsoft SQL Server\150\DTS\Extensions\Common\Jars)?

Deleting SQL Server files is not supported in general. In SSIS the log4j module is only used when dealing with Parquet or ORC file format. If customer does not use Parquet/ORC in their SSIS packages then the module will not be loaded.

2. Are the files impacted by CVE-2021-4104?

Microsoft has evaluated the use of the files shipped in "Program Files\Microsoft SQL Server\150\DTS\Extensions\Common\Jars\log4j-1.2.17.jar" and "Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\Binn\Polybase\Hadoop" in the context of SQL Server. They are not impacted by CVE-2021-4104. In SSIS the log4j module is only used when dealing with Parquet or ORC file format. If customer does not use Parquet/ORC in their SSIS packages then the module will not be loaded.


3. Is log4j 1.2.17 (1.X) that we use in SSIS has other vulnerability issue as described in [CVE-2019-17571 \(mitre.org\)](#)  ?


SSIS doesn't use the SocketServer feature as described in the [CVE - CVE-2019-17571 \(mitre.org\)](#) . So this CVE 2019-17571 is not applicable.

4. Will we release any patches to upgrade outdated versions of log4j?

For SSIS On-Prem: The fix for the Log4J issue is expected to be shipped with SQL Server 2019 CU 16 release.

For SSIS IR: Yes, we will ship it in the next IR release.

<Internal>: Refer to the below HOTFIX for more details - SSIS OnPrem [Hotfix 14482693:Hotfix for log4j2 Vulnerability to SQL Server SSIS](#) 


Refer to the [SQL Tiger Release](#)  for expected GA for SQL Server 2019 CU16


Questions around "why is old version shipped?", Give the answer above instead.

5. Will there be a fix for SQL Server 2017 and below supported versions?

SQL Server 2017 version and below doesn't install or use the Log4J components. Only SQL Server 2019 has Log4j components.

6. <Internal> When will these files be used ?


These files will be used when leveraging new capabilities introduced in SQL 2019: [What's new in SQL Server 2019 - SQL Server | Microsoft Docs](#) 

For SQL 2019 built-in installation, this is used by the HDFS File Destination component when choosing the ORC file format: [HDFS File Destination - SQL Server Integration Services \(SSIS\) | Microsoft Docs](#) . Flexible File components also use this, but they are installed by Azure Feature Pack for SSIS which is an OOB download.

7. For SSIS, through what installation does Log4j files get supplied and what is the expected ETA for the fix?
  - i. SQL Server 2019 setup - ETA for fix SQL Server 2019 CU16
  - ii. Azure Feature Pack 2019 - ETA for fix end of Feb 22
  - iii. Fix for VS2019/SSIS project extension / SSDT - Plan to kick off the release in Feb

Refer to [SQL Setup Workflow \(sharepoint.com\)](#)  for more questions.

## Azure Purview

There's has been no impact identified in any of the Purview service or component because of this vulnerability. More details [here](#). 

## Reference:

[CVE - CVE-2021-44228 \(mitre.org\)](#) 

[Microsoft's Response to CVE-2021-44228 Apache Log4j 2 – Microsoft Security Response Center](#) 

[Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation - Microsoft Security Blog](#) 

ICMs of other products:

SQL Server engine: <https://sqlbuvs01:8443/Main/SQL Server/ workitems#id=14428755& a=edit> 

Azure SQL VM - IaaS: <https://portal.microsofticm.com/imp/v3/incidents/details/277361507/home> 

Azure OSS PostgreSQL - Orcas ICM: <https://portal.microsofticm.com/imp/v3/incidents/details/277370703/home> 

Azure DataBricks: <https://portal.microsofticm.com/imp/v3/incidents/details/277474139/home> 

Synapse Spark: <https://portal.microsofticm.com/imp/v3/incidents/details/277546321/home> 

HDInsight: <https://portal.microsofticm.com/imp/v3/incidents/details/277408838/home> 

Azure Kubernetes: <https://portal.microsofticm.com/imp/v3/incidents/details/277313046/home> 

VMWare in Azure: <https://portal.microsofticm.com/imp/v3/incidents/details/277429647/home> 