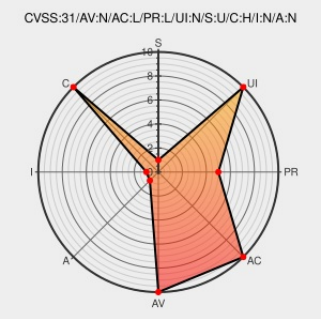
CVE-2021-26920

Published on: 07/02/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-26920

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Druid from Apache contain the following vulnerability:

In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource.

CVE-2021-26920 has been assigned by security@apache.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Druid** version **<= 0.20.2**

Vulnerability Patch/Work Around

Users can avoid the issue by upgrading to 0.21.0 or a higher version. In an earlier version than 0.21.0, when the user application wants to restrict the access to the local file system, it should disallow all InputSources that can read local files, that is the Local, HTTP, and HDFS InputSources.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [announce] 20210701 CVE-2021-26920: Apache Druid: The HTTP inputSource allows authent from other sources than intended
Pony Mail!	lists.apache.org text/html	MISC lists.apache.org/thread.html/r29e45561343cc5cf7d3290ee0b0e94e565faab19c20d022df9b5e29c%40%3
oss-security - CVE-2021-26920: Apache Druid: The HTTP inputSource allows authenticated users to read data from other sources than intended	www.openwall.com text/html	MLIST [oss-security] 20210702 CVE-2021-26920: Apache Druid: The HTTP inputSource allows authe from other sources than intended
Pony Mail!	lists.apache.org text/html	MLIST [druid-dev] 20210923 CVE-2021-36749: Apache Druid: The HTTP inputSource allows authenti from other sources than intended (incomplete fix of CVE-2021-26920)
oss-security - CVE-2021-36749: Apache Druid: The HTTP inputSource allows authenticated users to read data from other sources than intended (incomplete fix of CVE-2021-26920)	www.openwall.com text/html	MLIST [oss-security] 20210923 CVE-2021-36749: Apache Druid: The HTTP inputSource allows authe from other sources than intended (incomplete fix of CVE-2021-26920)
Pony Mail!	lists.apache.org text/html	MLIST [announce] 20210923 CVE-2021-36749: Apache Druid: The HTTP inputSource allows authent from other sources than intended (incomplete fix of CVE-2021-26920)

Related QID Numbers

980655 Java (maven) Security Update for org.apache.druid:druid (GHSA-793h-6f7r-6qvm)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Druid	All	All	All	All

cpe:2.3:a:apache:druid:*:*:*:*:*:*:*:*:

Discovery Credit

This issue was discovered by chybeta from the Security Team of Alibaba Cloud.

Social Mentions

Source	Title	Posted (UTC)
@oss_security	CVE-2021-26920: Apache Druid: The HTTP inputSource allows authenticated users to read data from other sources than… twitter.com/i/web/status/1…	2021-07-02 08:51:01

← Previous ID

Next ID→