



CVE-2021-36749

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-36749
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-24 10:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource does not validate the user-agent header, which allows an attacker to impersonate a trusted user and read sensitive data.

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
lists.apache.org/thread.html/rc9400a70d0ec5cdb8a3486fc5ddb0b5282961c0b63e764ab...
[announce] 20210923 CVE-2021-36749: Apache Druid: The HTTP inputSource allows authenticated users to read data from other sources than the one they are authorized to read from.
Pony Mail!
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was originally discovered by chybata from the Security Team of Alibaba Cloud.

LEGACY: ABKing and g0udan from the Security Team of Xiaomi discovered that it was still an issue after CVE-2021-26920.

Legacy QID Mappings

[980586](#) Java (maven) Security Update for org.apache.druid:druid (GHSA-9p5g-vg43-mj5r)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)