



CVE-2023-35797

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-35797
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-03 10:15:00 UTC
Updated	2023-07-13 23:15:00 UTC
Description	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Hive Provider. This issue affects Apache Airflow Hive Provider versions 2.10.0 through 2.10.1. An attacker can exploit this vulnerability to execute arbitrary code on the target system. The vulnerability is caused by the lack of input validation in the Hive Provider's <code>hive_conf</code> parameter. This issue affects Apache Airflow Hive Provider versions 2.10.0 through 2.10.1.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Apache-airflow-providers-apache-hive	All	All	All	All

References

Reference	Source
lists.apache.org/thread/30y19ok07fw52x5hnbkhwqo3ho0wwc1y	MISC
oss-security - CVE-2023-37415: Apache Airflow Apache Hive Provider: Improper Input Validation in Hive Provider with proxy_user	MISC
Sanitize beeline principal parameter by potiuk · Pull Request #31983 · apache/airflow · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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