



CVE-2022-40189

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

Summary

CVE	CVE-2022-40189
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-22 10:15:00 UTC
Updated	2022-11-29 13:57:00 UTC
Description	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Air

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Pig cli properties cannot be passed by connection extra by potiuk · Pull Request #27644 · apache/airflow · GitHub	MISC	github.com
lists.apache.org/thread/yxnfzfw2w9pj5s785k3rlyly4y44sd15	MISC	lists.apache
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Apache Airflow PMC wants to thank id_No2015429 of 3H Security Team for reporting the issue.

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

© [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](#)