Apache Airflow: OAuth Login CSRF — Missing State Parameter in Keycloak Auth Manager

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40948
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-18 14:16:10 UTC
Updated	2026-04-18 14:16:10 UTC
Description	The Keycloak authentication manager in `apache-airflow-providers-keycloak` did not generate or validate the OAuth 2.0 `sta

Risk And Classification

Problem Types: CWE-352 | CWE-352 CWE-352: Cross-Site Request Forgery (CSRF)

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Airflow	affected 0.0.1 0.7.0 semver	Not specified

References

Reference	Source	Link	Tags
github.com/apache/airflow/pull/64114	security@apache.org	github.com	
lists.apache.org/thread/kc0odpr70hbqhdb9ksnz42fkqz2xld9q	security@apache.org	lists.apache.org	
www.openwall.com/lists/oss-security/2026/04/17/14	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Haruki Oyama (Waseda University) (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report