



# Apache Airflow: API extra-links triggers XCom deserialization/class instantiation (Airflow 3.1.5)

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

## Summary

<b>CVE</b>	CVE-2026-25917
<b>State</b>	PUBLISHED
<b>Assigner</b>	apache
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-18 07:16:09 UTC
<b>Updated</b>	2026-04-22 14:16:36 UTC
<b>Description</b>	Dag Authors, who normally should not be able to execute code in the webserver context could craft XCom payload causing

## Risk And Classification

**Primary CVSS:** v3.1 7.2 HIGH from ADP

**CVSS:** 3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000660000 probability, percentile 0.203030000 (date 2026-04-21)

**Problem Types:** CWE-502 | CWE-502 CWE-502: Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

#### NVD Known Affected Configurations (CPE 2.3)

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Airflow	affected 3.2.0 semver	Not specified

#### References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/04/17/9	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing Li
lists.apache.org/thread/6whgpkqbh12rvpfmvcg8b0vwlv4hq3po	security@apache.org	<a href="http://lists.apache.org">lists.apache.org</a>	Mailing Li
github.com/apache/airflow/pull/61641	security@apache.org	<a href="http://github.com">github.com</a>	Issue Tra
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical

#### Vendor Comments And Credit

Discovery Credit

**CNA:** [Mahammad Huseynkhanli \(en\)](#)

**CNA:** [Amogh Desai \(en\)](#)

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](http://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)

