



Eclipse EDC: Consumer pull transfer token validation checks not applied

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

Summary

CVE	CVE-2024-8642
State	PUBLISHED
Assigner	eclipse
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-11 14:15:14 UTC
Updated	2026-04-29 01:00:01 UTC
Description	In Eclipse Dataspace Components, from version 0.5.0 and before version 0.9.0, the ConsumerPullTransferTokenValidation

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from emo@eclipse.org

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:L/U:Gr
een

Problem Types: CWE-303 | CWE-305 | CWE-287 | CWE-303 CWE-303 | CWE-305 CWE-305

Version	Source	Type	Score	Severity	Vector
4.0	emo@eclipse.org	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/C..
4.0	CNA	CVSS	5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/RE:L/..
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:L/U:Gr
een

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Eclipse Dataspace Components	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Eclipse Foundation	Eclipse EDC Connector	affected 0.5.0 0.9.0 semver	Not specified
ADP	Eclipse Foundation	Edc	affected 0.5.0 0.9.0 custom	Not specified

References

Reference	Source	Link	Tags
gitlab.eclipse.org/security/cve-assignement/-/issues/28	emo@eclipse.org	gitlab.eclipse.org	Issue Tracking
github.com/eclipse-edc/Connector/releases/tag/v0.9.0	emo@eclipse.org	github.com	Release Notes
github.com/eclipse-edc/Connector/commit/04899e91dcd4a407db4eb7af3e7b6ff...	emo@eclipse.org	github.com	Patch
gitlab.eclipse.org/security/vulnerability-reports/-/issues/234	emo@eclipse.org	gitlab.eclipse.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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