



# CVE-2025-40571

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

## Summary

<b>CVE</b>	CVE-2025-40571
<b>State</b>	PUBLISHED
<b>Assigner</b>	siemens
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-05-13 10:15:26 UTC
<b>Updated</b>	2026-04-14 09:16:34 UTC
<b>Description</b>	A vulnerability has been identified in Mendix OIDC SSO (Mendix 10.12 compatible) (All versions < V4.0.1), Mendix OIDC S

## Risk And Classification

**Primary CVSS:** v4.0 2.1 LOW from productcert@siemens.com

**CVSS:**4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/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:X/U:X

**EPSS:** 0.001450000 probability, percentile 0.349600000 (date 2026-04-15)

**Problem Types:** CWE-266 | CWE-266 CWE-266: Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
4.0	productcert@siemens.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/S
4.0	CNA	DECLARED	2.1	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/S
3.1	productcert@siemens.com	Secondary	2.2	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	2.2	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

None

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/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:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Siemens	Mendix OIDC SSO Mendix 10.12 Compatible	affected V4.0.1 custom	Not specified
CNA	Siemens	Mendix OIDC SSO Mendix 9 Compatible	affected V3.3.1 custom	Not specified
CNA	Siemens	Mendix OIDC SSO V4.2 Mendix 10 Compatible	affected V4.2.1 custom	Not specified
CNA	Siemens	Mendix OIDC SSO V4.3 Mendix 10 Compatible	affected * custom	Not specified

## References

Reference	Source	Link	Tags
<a href="https://cert-portal.siemens.com/productcert/html/ssa-726617.html">cert-portal.siemens.com/productcert/html/ssa-726617.html</a>	productcert@siemens.com	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

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