



# CVE-2025-4655

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

## Summary

<b>CVE</b>	CVE-2025-4655
<b>State</b>	PUBLISHED
<b>Assigner</b>	Liferay
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-08-09 05:15:29 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	SSRF vulnerability in FreeMarker templates in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from security@liferay.com

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

**Problem Types:** CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security@liferay.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N/E:X
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N
3.1	nvd@nist.gov	Primary	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

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

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

None

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Digital Experience Platform	All	All	All	All
Application	Liferay	Digital Experience Platform	All	All	All	All
Application	Liferay	Digital Experience Platform	All	All	All	All
Application	Liferay	Digital Experience Platform	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	<a href="#">Liferay</a>	<a href="#">Portal</a>	affected 7.4.0 7.4.3.132 maven	Not specified
CNA	<a href="#">Liferay</a>	<a href="#">DXP</a>	affected 7.4.13 7.4.13-u92 maven	Not specified
CNA	<a href="#">Liferay</a>	<a href="#">DXP</a>	affected 2024.Q1.1 2024.Q1.15 maven	Not specified
CNA	<a href="#">Liferay</a>	<a href="#">DXP</a>	affected 2024.Q2.0 2024.Q2.13 maven	Not specified
CNA	<a href="#">Liferay</a>	<a href="#">DXP</a>	affected 2024.Q3.1 2024.Q3.13 maven	Not specified
CNA	<a href="#">Liferay</a>	<a href="#">DXP</a>	affected 2024.Q4.0 2024.Q4.7 maven	Not specified
CNA	<a href="#">Liferay</a>	<a href="#">DXP</a>	affected 2025.Q1.0 2025.Q1.5 maven	Not specified

## References

Reference	Source	Link	Tags
<a href="https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/...">liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/...</a>	<a href="mailto:security@liferay.com">security@liferay.com</a>	<a href="https://liferay.dev">liferay.dev</a>	Vendor Advisory
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

## Vendor Comments And Credit

### Discovery Credit

**CNA:** José Ricardo (ricard0x) (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](https://cve.report/api)

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