CVE-2025-4655

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

Summary

CVE	CVE-2025-4655
State	PUBLISHED
Assigner	Liferay
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-08-09 05:15:29 UTC
Updated	2026-04-29 01:00:01 UTC
Description	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/MSC:X/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/MSC:X/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	Liferay	Portal	affected 7.4.0 7.4.3.132 maven	Not specified
CNA	Liferay	DXP	affected 7.4.13 7.4.13-u92 maven	Not specified
CNA	Liferay	DXP	affected 2024.Q1.1 2024.Q1.15 maven	Not specified
CNA	Liferay	DXP	affected 2024.Q2.0 2024.Q2.13 maven	Not specified
CNA	Liferay	DXP	affected 2024.Q3.1 2024.Q3.13 maven	Not specified
CNA	Liferay	DXP	affected 2024.Q4.0 2024.Q4.7 maven	Not specified
CNA	Liferay	DXP	affected 2025.Q1.0 2025.Q1.5 maven	Not specified

References

Reference	Source	Link	Tags
liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/...	security@liferay.com	liferay.dev	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: José Ricardo (ricard0x) (en)

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