



CVE-2023-42628

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-42628
State	PUBLIC
Assigner	security@liferay.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-17 12:15:00 UTC
Updated	2023-11-10 03:15:00 UTC
Description	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0.0 through 7.4.3.87.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Digital Experience Platform	7.0	-	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_1	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_10	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_11	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_12	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_13	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_14	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_15	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_16	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_17	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_18	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_19	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_2	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_20	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_21	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_22	All	All
Application	Liferay	Digital Experience Platform	7.0	fix_pack_23	All	All

Application	Liferay	Digital Experience Platform	7.4	update21	All	All
Application	Liferay	Digital Experience Platform	7.4	update34	All	All
Application	Liferay	Digital Experience Platform	7.4	update36	All	All
Application	Liferay	Digital Experience Platform	7.4	update41	All	All
Application	Liferay	Digital Experience Platform	7.4	update48	All	All
Application	Liferay	Digital Experience Platform	7.4	update50	All	All
Application	Liferay	Digital Experience Platform	7.4	update52	All	All
Application	Liferay	Digital Experience Platform	7.4	update62	All	All
Application	Liferay	Digital Experience Platform	7.4	update67	All	All
Application	Liferay	Digital Experience Platform	7.4	update76	All	All
Application	Liferay	Digital Experience Platform	7.4	update81	All	All
Application	Liferay	Digital Experience Platform	7.4	update82	All	All
Application	Liferay	Digital Experience Platform	7.4	update83	All	All
Application	Liferay	Digital Experience Platform	7.4	update84	All	All
Application	Liferay	Digital Experience Platform	7.4	update85	All	All
Application	Liferay	Digital Experience Platform	7.4	update86	All	All
Application	Liferay	Liferay Portal	All	All	All	All

References

Reference	Source	Link	Tags
Persistent cross-site scripting vulnerabilities in Liferay Portal Pentagrid AG		www.pentagrid.ch	
CVE-2023-42628 XSS with child wiki pages - Liferay	MISC	liferay.dev	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[731005](#) Liferay Portal Stored Cross-Site Scripting (XSS) Vulnerability

© [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

