



# CVE-2022-42118

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

## Summary

<b>CVE</b>	CVE-2022-42118
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-15 01:15:00 UTC
<b>Updated</b>	2022-11-17 14:42:00 UTC
<b>Description</b>	A Cross-site scripting (XSS) vulnerability in the Portal Search module in Liferay Portal 7.1.0 through 7.4.2, and Liferay DXP

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	-	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_1	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_10	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_11	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_12	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_13	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_14	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_15	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_16	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_17	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_18	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_19	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_2	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_20	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_21	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_22	All	All
Application	<a href="#">Liferay</a>	<a href="#">Dxp</a>	7.1	fix_pack_23	All	All

Application	Liferay	Dxp	7.1	fix_pack_24	All	All
Application	Liferay	Dxp	7.1	fix_pack_25	All	All
Application	Liferay	Dxp	7.1	fix_pack_3	All	All
Application	Liferay	Dxp	7.1	fix_pack_4	All	All
Application	Liferay	Dxp	7.1	fix_pack_5	All	All
Application	Liferay	Dxp	7.1	fix_pack_6	All	All
Application	Liferay	Dxp	7.1	fix_pack_7	All	All
Application	Liferay	Dxp	7.1	fix_pack_8	All	All
Application	Liferay	Dxp	7.1	fix_pack_9	All	All
Application	Liferay	Dxp	7.2	-	All	All
Application	Liferay	Dxp	7.2	fix_pack_1	All	All
Application	Liferay	Dxp	7.2	fix_pack_10	All	All
Application	Liferay	Dxp	7.2	fix_pack_11	All	All
Application	Liferay	Dxp	7.2	fix_pack_12	All	All
Application	Liferay	Dxp	7.2	fix_pack_13	All	All
Application	Liferay	Dxp	7.2	fix_pack_14	All	All
Application	Liferay	Dxp	7.2	fix_pack_2	All	All
Application	Liferay	Dxp	7.2	fix_pack_3	All	All
Application	Liferay	Dxp	7.2	fix_pack_4	All	All
Application	Liferay	Dxp	7.2	fix_pack_5	All	All
Application	Liferay	Dxp	7.2	fix_pack_6	All	All
Application	Liferay	Dxp	7.2	fix_pack_7	All	All
Application	Liferay	Dxp	7.2	fix_pack_8	All	All
Application	Liferay	Dxp	7.2	fix_pack_9	All	All
Application	Liferay	Dxp	7.3	-	All	All
Application	Liferay	Dxp	7.3	sp1	All	All
Application	Liferay	Dxp	7.3	sp2	All	All
Application	Liferay	Liferay Portal	All	All	All	All

## References

Reference	Source	Link	Tags
Digital Experience Software Tailored to Your Needs   Liferay	MISC	<a href="https://liferay.com">liferay.com</a>	
CVE-2022-42118 Reflected XSS with `tag` in Search	MISC	<a href="https://portal.liferay.dev">portal.liferay.dev</a>	
[LPE-17342] LSV-906: Reflected XSS with `tag` in Search - Liferay Issues	MISC	<a href="https://issues.liferay.com">issues.liferay.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

731102 Liferay Portal Multiple Cross-Site Scripting (XSS) Vulnerabilities

© [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](#).

**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)