



# CVE-2021-38264

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

## Summary

<b>CVE</b>	CVE-2021-38264
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-03 00:15:00 UTC
<b>Updated</b>	2022-06-05 03:51:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.4.0 and 7.4.1 allows remote attackers

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Liferay Portal	7.4.0	All	All	All
Application	Liferay	Liferay Portal	7.4.1	-	All	All

## References

Reference	Source	Link	Tags
CVE-2021-38264 Reflected XSS with `keywords` in Search	MISC	<a href="https://portal.liferay.dev">portal.liferay.dev</a>	
Digital Experience Software Tailored to Your Needs   Liferay	MISC	<a href="https://liferay.com">liferay.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.

## Legacy QID Mappings

[730488](#) Liferay Portal Reflected Cross-Site Scripting (XSS) Vulnerability

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**