



# CVE-2021-35463

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

## Summary

<b>CVE</b>	CVE-2021-35463
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-04 14:15:00 UTC
<b>Updated</b>	2021-08-11 00:09:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.4.0 allows remote attackers to inject

## 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

## References

Reference	Source	Link	Tags
CVE-2021-35463 Reflected XSS with `keywords` in Search	CONFIRM	<a href="https://portal.liferay.dev">portal.liferay.dev</a>	
CVE-2021-33339 Stored XSS with Site name in Fragment portlet	CONFIRM	<a href="https://portal.liferay.dev">portal.liferay.dev</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.

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

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](#)**