



CVE-2022-42125

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

Summary

CVE	CVE-2022-42125
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-15 01:15:00 UTC
Updated	2022-11-18 16:51:00 UTC
Description	Zip slip vulnerability in FileUtil.unzip in Liferay Portal 7.4.3.5 through 7.4.3.35 and Liferay DXP 7.4 update 1 through update

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Digital Experience Platform	7.4	update1	All	All
Application	Liferay	Digital Experience Platform	7.4	update34	All	All
Application	Liferay	Liferay Portal	All	All	All	All

References

Reference	Source	Link	Tags
Digital Experience Software Tailored to Your Needs Liferay	MISC	liferay.com	
[LPE-17517] LSV-1038: Zip slip vulnerability in FileUtil.unzip - Liferay Issues	MISC	issues.liferay.com	
CVE-2022-42125 Zip slip vulnerability in FileUtil.unzip	MISC	portal.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.

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

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

CVE.report and Source URL Uptime Status status.cve.report