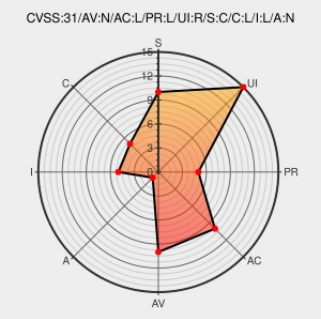
CVE-2022-42114

Published on: Not Yet Published

Last Modified on: 10/20/2022 06:09:00 PM UTC

CVE-2022-42114

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dxp from Liferay contain the following vulnerability:

A Cross-site scripting (XSS) vulnerability in the Role module's edit role assignees page in Liferay Portal 7.4.0 through 7.4.3.36, and Liferay DXP 7.4 before update 37 allows remote attackers to inject arbitrary web script or HTML.

CVE-2022-42114 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Digital Experience Software Tailored to Your Needs | Liferay	liferay.com text/html	MISC liferay.com
CVE-2022-42114 Stored XSS with role key in edit assignees page	portal.liferay.dev text/html	MISC portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-42114

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A Cross-site scripting (XSS) vulnerability in the Role module's edit role assignees page in Liferay Portal 7.4.0 thro…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Dxp	All	All	All	All
Application	Liferay	Dxp	7.4	ga1	All	All
Application	Liferay	Dxp	7.4	update_1	All	All
Application	Liferay	Dxp	7.4	update_10	All	All
Application	Liferay	Dxp	7.4	update_11	All	All
Application	Liferay	Dxp	7.4	update_12	All	All
Application	Liferay	Dxp	7.4	update_13	All	All
Application	Liferay	Dxp	7.4	update_14	All	All
Application	Liferay	Dxp	7.4	update_15	All	All
Application	Liferay	Dxp	7.4	update_16	All	All
Application	Liferay	Dxp	7.4	update_17	All	All
Application	Liferay	Dxp	7.4	update_18	All	All
Application	Liferay	Dxp	7.4	update_19	All	All
Application	Liferay	Dxp	7.4	update_2	All	All
Application	Liferay	Dxp	7.4	update_20	All	All
Application	Liferay	Dxp	7.4	update_21	All	All
Application	Liferay	Dxp	7.4	update_22	All	All
Application	Liferay	Dxp	7.4	update_23	All	All
Application	Liferay	Dxp	7.4	update_24	All	All
Application	Liferay	Dxp	7.4	update_25	All	All
Application	Liferay	Dxp	7.4	update_26	All	All
Application	Liferay	Dxp	7.4	update_27	All	All
Application	Liferay	Dxp	7.4	update_28	All	All
Application	Liferay	Dxp	7.4	update_29	All	All
Application	Liferay	Dxp	7.4	update_3	All	All
Application	Liferay	Dxp	7.4	update_30	All	All
Application	Liferay	Dxp	7.4	update_31	All	All
Application	Liferay	Dxp	7.4	update_32	All	All
Application	Liferay	Dxp	7.4	update_33	All	All
Application	Liferay	Dxp	7.4	update_34	All	All

Application	Liferay	Dxp	7.4	update_34	All	All
Application	Liferay	Dxp	7.4	update_35	All	All
Application	Liferay	Dxp	7.4	update_36	All	All
Application	Liferay	Dxp	7.4	update_4	All	All
Application	Liferay	Dxp	7.4	update_5	All	All
Application	Liferay	Dxp	7.4	update_6	All	All
Application	Liferay	Dxp	7.4	update_7	All	All
Application	Liferay	Dxp	7.4	update_8	All	All
Application	Liferay	Dxp	7.4	update_9	All	All
Application	Liferay	Liferay Portal	All	All	All	All

cpe:2.3:a:liferay:dxp:*:*:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:ga1:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_1:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_10:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_11:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_12:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_13:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_14:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_15:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_16:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_17:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_18:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_19:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_2:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_20:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_21:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_22:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_23:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_24:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_25:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_26:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_27:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_28:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_29:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_3:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_30:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_31:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_32:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_33:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_34:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_35:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_36:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_4:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_5:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_6:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_7:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_8:*:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.4:update_9:*:*:*:*:*:*:

cpe:2.3:a:liferay:liferay_portal:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-42114 : A Cross-site scripting #XSS vulnerability in the Role module's edit role assignees page in Lifer… twitter.com/i/web/status/1…	2022-10-18 21:26:29
@LinInfoSec	Liferay - CVE-2022-42114: portal.liferay.dev/learn/security…	2022-10-19 00:00:12

← Previous ID

Next ID→

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