



CVE-2022-28977

Published on: Not Yet Published

Last Modified on: 09/23/2022 05:55:00 PM UTC

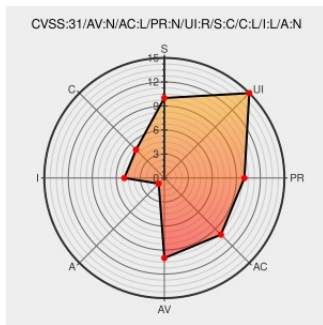
CVE-2022-28977

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Dxp](#) from [Liferay](#) contain the following vulnerability:

HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through 101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) `redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect.

CVE-2022-28977 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	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-2022-28977 HtmlUtil.escapeRedirect circumvention with multiple forward slash	portal.liferay.dev text/html	MISC portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28977-htmlutil.escaperedirect-circumvention-with-multiple-forward-slash

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)



Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Dxp	7.0	-	All	All
Application	Liferay	Dxp	7.0	fix_pack_100	All	All
Application	Liferay	Dxp	7.0	fix_pack_101	All	All
Application	Liferay	Dxp	7.0	fix_pack_91	All	All
Application	Liferay	Dxp	7.0	fix_pack_92	All	All
Application	Liferay	Dxp	7.0	fix_pack_93	All	All
Application	Liferay	Dxp	7.0	fix_pack_94	All	All
Application	Liferay	Dxp	7.0	fix_pack_95	All	All
Application	Liferay	Dxp	7.0	fix_pack_96	All	All
Application	Liferay	Dxp	7.0	fix_pack_97	All	All
Application	Liferay	Dxp	7.0	fix_pack_98	All	All
Application	Liferay	Dxp	7.0	fix_pack_99	All	All
Application	Liferay	Dxp	7.1	-	All	All
Application	Liferay	Dxp	7.1	fix_pack_17	All	All
Application	Liferay	Dxp	7.1	fix_pack_18	All	All
Application	Liferay	Dxp	7.1	fix_pack_19	All	All
Application	Liferay	Dxp	7.1	fix_pack_20	All	All
Application	Liferay	Dxp	7.1	fix_pack_21	All	All
Application	Liferay	Dxp	7.1	fix_pack_22	All	All
Application	Liferay	Dxp	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	7.2	-	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_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



- cpe:2.3:a:liferay:dxp:7.0:-:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_100:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_101:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_91:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_92:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_93:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_94:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_95:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_96:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_97:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_98:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.0:fix_pack_99:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:-:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_17:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_18:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_19:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_20:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_21:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_22:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_23:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_24:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.1:fix_pack_25:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.2:-:*:*:*:*:*:
- cpe:2.3:a:liferay:dxp:7.2:fix_pack_10:*:*:*:*:*:

cpe:2.3:a:liferay:dxp:7.2:fix_pack_11:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_12:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_13:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_14:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_5:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_6:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_7:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_8:~::~::~:
cpe:2.3:a:liferay:dxp:7.2:fix_pack_9:~::~::~:
cpe:2.3:a:liferay:dxp:7.3:-:~::~::~:
cpe:2.3:a:liferay:dxp:7.3:sp1:~::~::~:
cpe:2.3:a:liferay:dxp:7.3:sp2:~::~::~:
cpe:2.3:a:liferay:liferay_portal:~::~::~:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-28977 : HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 thr... twitter.com/i/web/status/1...	2022-09-22 01:06:04
 /r/netcve	CVE-2022-28977	2022-09-22 02:38:19

[← Previous ID](#) [Next ID →](#)

© CVE.report 2022   | 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](#).

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