

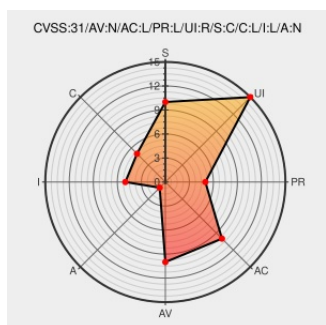


CVE-2023-27474

Published on: Not Yet Published

Last Modified on: 03/13/2023 05:52:00 PM UTC

CVE-2023-27474 - advisory for GHSA-4hmq-ggrm-qfc6

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Directus](#) from [Rangerstudio](#) contain the following vulnerability:

Directus is a real-time API and App dashboard for managing SQL database content. Instances relying on an allow-listed reset URL are vulnerable to an HTML injection attack through the use of query parameters in the reset URL. An attacker could exploit this to email users urls to the servers domain but which may contain malicious code.

The problem has been resolved and released under version 9.23.0. People relying on a custom password reset URL should upgrade to 9.23.0 or later, or remove the custom reset url from the configured allow list. Users are advised to upgrade. Users unable to upgrade may disable the custom reset URL allow list as a workaround.

CVE-2023-27474 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [directus](#) - **directus** version = < 9.23.0

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
Fix url encoding query parameters and added tests by tofran · Pull Request #17120 · directus/directus · GitHub	github.com text/html	MISC github.com/directus/directus/pull/17120
HTML Injection in Password Reset email to custom Reset URL · Advisory · directus/directus · GitHub	github.com text/html	MISC github.com/directus/directus/security/advisories/GHSA-4hmq-ggrm-qfc6

Password reset improperly handles url-encoded query parameters
in reset_url · Issue #17119 · directus/directus · GitHub

github.com
text/html

MISC github.com/directus/directus/issues/17119

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	Rangerstudio	Directus	All	All	All	All
cpe:2.3:a:rangerstudio:directus:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-27474 : Directus is a real-time API and App dashboard for managing SQL database content. Instances relying... twitter.com/i/web/status/1...	2023-03-06 17:06:08
 /r/netcve	CVE-2023-27474	2023-03-06 18:38:07
 /r/Team_IT_Security	CVE-2023-27474 Directus up to 9.22.x Query Parameter cross site scripting (ID 17119)	2023-03-31 22:06:06

← Previous ID

Next ID →

© CVE.report 2023   |

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](#)