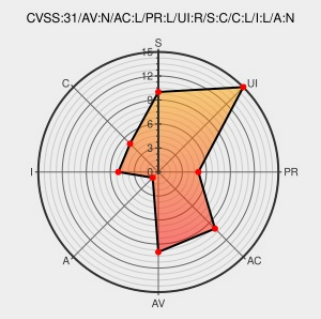
CVE-2023-27474

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 improperlly handles url-encoded query parameters in reset_url · Issue #17119 · directus/directus · GitHub	github.com text/html	MISC github.com/directus/directus/issues/17119

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→