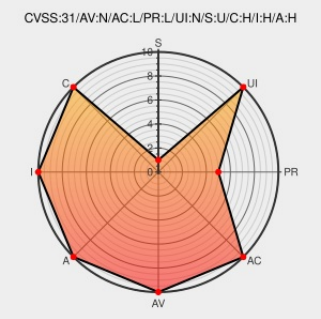
CVE-2022-23510

Published on: Not Yet Published

Last Modified on: 12/13/2022 03:07:00 PM UTC

CVE-2022-23510 - advisory for GHSA-6jqm-3c9g-pch7

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



Certain versions of Cube.js from Cube contain the following vulnerability:

cube-js is a headless business intelligence platform. In version 0.31.23 all authenticated Cube clients could bypass SQL row-level security and run arbitrary SQL via the newly introduced /v1/sql-runner endpoint. This issue has been resolved in version 0.31.24. Users are advised to either upgrade to 0.31.24 or to downgrade to 0.31.22. There are no known workarounds for this vulnerability.

CVE-2022-23510 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **cube-js** - **cube.js** version **= = 0.31.23**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
Revert "chore(cubejs-api-gateway): added endpoint to run sql query di… · cube-js/cube.js@f1140de · GitHub	github.com text/html	MISC github.com/cube-js/cube.js/commit/f1140de508e359970ac82b50bae1c4bf152f6041
Revert "feat(api-gateway, server-core): Added dataSources list to ext… · cube-js/cube.js@3c61467 · GitHub	github.com text/html	MISC github.com/cube-js/cube.js/commit/3c614674fed6ca17df08bbba8c835ef110167570
Row level security bypass · Advisory · cube-js/cube.js · GitHub	github.com text/html	MISC github.com/cube-js/cube.js/security/advisories/GHSA-6jqm-3c9g-pch7

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	Cube	Cube.js	0.31.23	All	All	All

cpe:2.3:a:cube:cube.js:0.31.23:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23510 : cube-js is a headless business intelligence platform. In version 0.31.23 all authenticated Cube cl… twitter.com/i/web/status/1…	2022-12-09 23:05:29
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-23510 cube-js is a headless business intelligence platform. In version… twitter.com/i/web/status/1…	2022-12-09 23:56:00
/r/netcve	CVE-2022-23510	2022-12-10 00:38:23

← Previous ID

Next ID→

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