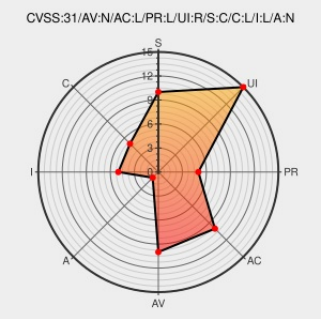
CVE-2023-25572

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:09:00 AM UTC

CVE-2023-25572 - advisory for GHSA-5jcr-82fh-339v

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



Certain versions of Ra-ui-materialui from Marmelab contain the following vulnerability:

react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior to versions 3.19.12 and 4.7.6, along with ra-ui-materialui prior to 3.19.12 and 4.7.6, are vulnerable to cross-site scripting. All React applications built with react-admin and using the `<RichTextField>` are affected. `<RichTextField>` outputs the field value using `dangerouslySetInnerHTML` without client-side sanitization. If the data isn't sanitized server-side, this opens a possible cross-site scripting (XSS) attack. Versions 3.19.12 and 4.7.6 now use `DOMPurify` to escape the HTML before outputting it with React and `dangerouslySetInnerHTML`. Users who already sanitize HTML data server-side do not need to upgrade. As a workaround, users may replace the `<RichTextField>` by a custom field doing sanitization by hand.

CVE-2023-25572 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **marmelab** - **react-admin** version **= < 3.19.12**

Affected Vendor/Software: **marmelab** - **react-admin** version **= >= 4.0.0, < 4.7.6**

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

Cross-Site-Scripting attack on RichTextField · Advisory · marmelab/react-admin · GitHub	github.com text/html	MISC github.com/marmelab/react-admin/security/advisories/GHSA-5jcr-82fh-339v
Fix `` XSS vulnerability by fzaninotto · Pull Request #8645 · marmelab/react-admin · GitHub	github.com text/html	MISC github.com/marmelab/react-admin/pull/8645
Release 3.19.12 · marmelab/react-admin · GitHub	github.com text/html	MISC github.com/marmelab/react-admin/releases/tag/v3.19.12
Release 4.7.6 · marmelab/react-admin · GitHub	github.com text/html	MISC github.com/marmelab/react-admin/releases/tag/v4.7.6
Fix `` XSS vulnerability by fzaninotto · Pull Request #8644 · marmelab/react-admin · GitHub	github.com text/html	MISC github.com/marmelab/react-admin/pull/8644

There are currently no QIDs associated with this CVE

Exploit/POC from Github

react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Marmelab	Ra-ui-materialui	All	All	All	All
Application	Marmelab	React-admin	All	All	All	All

cpe:2.3:a:marmelab:ra-ui-materialui:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:marmelab:react-admin:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25572 : react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs.… twitter.com/i/web/status/1…	2023-02-13 21:05:57
/r/netcve	CVE-2023-25572	2023-02-13 21:38:50

← Previous ID

Next ID→

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