



# CVE-2023-25572

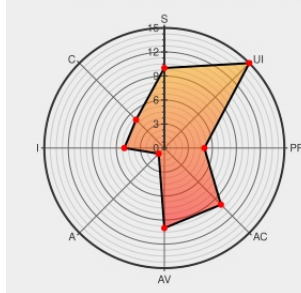
Published on: Not Yet Published

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](#)

CVSS:31/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N



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    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>LOW</b>          | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

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

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](mailto:comment@cve.report).

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                                              | <a href="#">Marmelab</a> | <a href="#">Ra-ui-materialui</a> | All     | All    | All     | All      |
| Application                                              | <a href="#">Marmelab</a> | <a href="#">React-admin</a>      | 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.... <a href="#">twitter.com/i/web/status/1...</a> | 2023-02-13 21:05:57 |
|  /r/netcve  | <a href="#">CVE-2023-25572</a>                                                                                                                                       | 2023-02-13 21:38:50 |

[← Previous ID](#)

[Next ID →](#)

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](#)