

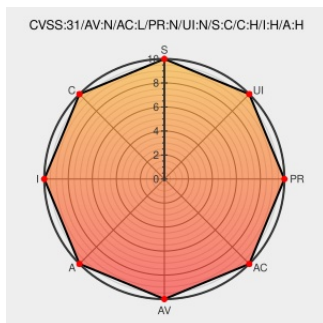


CVE-2022-36010

Published on: Not Yet Published

Last Modified on: 08/16/2022 05:47:00 PM UTC

CVE-2022-36010 - advisory for GHSA-j3rv-w43q-f9x2

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

Certain versions of [React Editable Json Tree](#) from [React Editable Json Tree Project](#) contain the following vulnerability:

This library allows strings to be parsed as functions and stored as a specialized component, [`JsonFunctionValue`] (<https://github.com/oxyno-zeta/react-editable-json->

[tree/blob/09a0ca97835b0834ad054563e2fddc6f22bc5d8c/src/components/JsonFunctionValue](https://github.com/oxyno-zeta/react-editable-json-tree/blob/09a0ca97835b0834ad054563e2fddc6f22bc5d8c/src/components/JsonFunctionValue) To do this, Javascript's [`eval`] (https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/eval) function is used to execute strings that begin with "function" as Javascript. This unfortunately could allow arbitrary code to be executed if it exists as a value within the JSON structure being displayed. Given that this component may often be used to display data from arbitrary, untrusted sources, this is extremely dangerous. One important note is that users who have defined a custom [`onSubmitValueParser`] (<https://github.com/oxyno-zeta/react-editable-json-tree/tree/09a0ca97835b0834ad054563e2fddc6f22bc5d8c#onsubmitvalueparser>) callback prop on the [`JsonTree`] (<https://github.com/oxyno-zeta/react-editable-json-tree/blob/09a0ca97835b0834ad054563e2fddc6f22bc5d8c/src/JsonTree.js>) component should be `***unaffected***`. This vulnerability exists in the default `onSubmitValueParser` prop which calls [`parse`] (<https://github.com/oxyno-zeta/react-editable-json-tree/blob/master/src/utils/parse.js#L30>). Prop is added to `JsonTree` called `allowFunctionEvaluation`. This prop will be set to `true` in v2.2.2, which allows upgrade without losing backwards-compatibility. In v2.2.2, we switched from using `eval` to using [`Function`] (https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Function) to construct anonymous functions. This is better than `eval` for the following reasons: - Arbitrary code should not be able to execute immediately, since the `Function` constructor explicitly *only creates* anonymous functions - Functions are created without local closures, so they only have access to the global scope If you use: - `**Version <2.2.2**`, you must upgrade as soon as possible. - `**Version ^2.2.2**`, you must explicitly set `JsonTree`'s `allowFunctionEvaluation` prop to `false` to fully mitigate this vulnerability. - `**Version >=3.0.0**`, `allowFunctionEvaluation` is

already set to `false` by default, so no further steps are necessary.

CVE-2022-36010 has been assigned by  security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software:  **oxyno-zeta - react-editable-json-tree** version < 2.2.2

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
Release 2.2.2 · oxyno-zeta/react-editable-json-tree · GitHub	github.com text/html	 MISC github.com/oxyno-zeta/react-editable-json-tree/releases/tag/2.2.2
Arbitrary code execution via function parsing · Advisory · oxyno-zeta/react-editable-json-tree · GitHub	github.com text/html	 CONFIRM github.com/oxyno-zeta/react-editable-json-tree/security/advisories/GHSA-j3rv-w43q-f9x2

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	React Editable Json Tree Project	React Editable Json Tree	All	All	All	All
cpe:2.3:a:react_editable_json_tree_project:react_editable_json_tree:*.***.*:node.js:*.**:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-36010 : This library allows strings to be parsed as functions and stored as a specialized component, [Jso... twitter.com/i/web/status/1...	2022-08-15 18:38:33
 @Robo Alerts	Potentially Critical CVE Detected! CVE-2022-36010 This library allows strings to be parsed as functions and stored... twitter.com/i/web/status/1...	2022-08-15 20:56:00

oxyno-zeta	Reactions and status: github.com/oxyno-zeta/rea...	2022-08-15 21:00:16
 /r/netcve	CVE-2022-36010	2022-08-15 19:38:18

[← 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](#)