



CVE-2021-43801

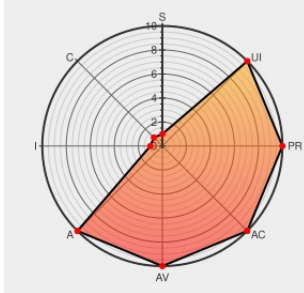
Published on: Not Yet Published

Last Modified on: 12/15/2021 09:46:00 PM UTC

CVE-2021-43801 - advisory for GHSA-273r-rm8g-7f3x

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

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



Certain versions of [Mercurius](#) from [Mercurius Project](#) contain the following vulnerability:

Mercurius is a GraphQL adapter for Fastify. Any users from Mercurius@8.10.0 to 8.11.1 are subjected to a denial of service attack by sending a malformed JSON to `/graphql` unless they are using a custom error handler. The vulnerability has been fixed in <https://github.com/mercurius-js/mercurius/pull/678> and shipped as v8.11.2. As a workaround users may use a custom error handler.

CVE-2021-43801 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [mercurius-js](#) - **mercurius** version `>= 8.10.0, < 8.11.2`

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

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

Uncaught Exception in mercurius · Advisory · mercurius-js/mercurius · GitHub	github.com text/html	CONFIRM github.com/mercurius-js/mercurius/security/advisories/GHSA-273r-rm8g-7f3x
Fix regression in handling badly formed JSON by mcollina · Pull Request #678 · mercurius-js/mercurius · GitHub	github.com text/html	MISC github.com/mercurius-js/mercurius/pull/678/commits/732b2f895312da8deadd7b173dcd2d141d54b223
Context can be undefined in the error handler · Issue #677 · mercurius-js/mercurius · GitHub	github.com text/html	MISC github.com/mercurius-js/mercurius/issues/677

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	Mercurius Project	Mercurius	All	All	All	All
cpe:2.3:a:mercurius_project:mercurius:*:*:*:*:node.js:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2021-43801	2021-12-13 20:38:49

[← Previous ID](#)

[Next ID →](#)