

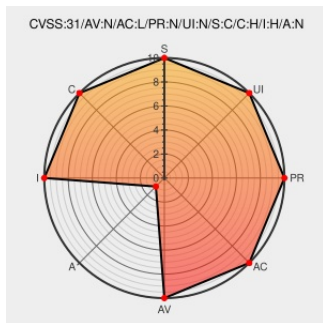


CVE-2021-21321

Published on: 03/01/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:58 PM UTC

CVE-2021-21321 - advisory for GHSA-qmw8-3v4g-gwj4

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

Certain versions of [Fastify-reply-from](#) from [Fastify-reply-from Project](#) contain the following vulnerability:

fastify-reply-from is an npm package which is a fastify plugin to forward the current http request to another server. In fastify-reply-from before version 4.0.2, by crafting a specific URL, it is possible to escape the prefix of the proxied backend service. If the base url of the proxied server is "/pub/", a user expect that accessing "/priv" on the target service would not be possible. In affected versions, it is possible. This is fixed in version 4.0.2.

CVE-2021-21321 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: fastify - fastify-reply-from version < 4.0.2

CVSS3 Score: **10 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Type	Link
-------------	------	------

Description	Tags	Link
fastify-reply-from - npm	Product Third Party Advisory www.npmjs.com text/html	 MISC www.npmjs.com/package/fastify-reply-from
Merge pull request from GHSA-qmw8-3v4g-gwj4 · fastify/fastify-reply-from@dea227d · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/fastify/fastify-reply-from/commit/dea227dda606900cc01870d08541b4dcc69d3889
Prefix escape · Advisory · fastify/fastify-reply-from · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/fastify/fastify-reply-from/security/advisories/GHSA-qmw8-3v4g-gwj4

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.

Related QID Numbers

982930 Nodejs (npm) Security Update for fastify-reply-from (GHSA-qmw8-3v4g-gwj4)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastify-reply-from Project	Fastify-reply-from	All	All	All	All
Application	Fastify-reply-from Project	Fastify-reply-from	All	All	All	All
cpe:2.3:a:fastify-reply-from_project:fastify-reply-from:*:*:*:*:node.js:*:						
cpe:2.3:a:fastify-reply-from_project:fastify-reply-from:*:*:*:*:node.js:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @M157q_News_RSS	Addressing Input Sanitization Bugs and CVE 2021-21321 hackernoon.com/addressing-inp... CVE 2021-21321 indicates a vulnerabil... twitter.com/i/web/status/1...	2021-06-23 16:45:58
 @hackernoon	"Addressing Input Sanitization Bugs and CVE 2021-21321" hackernoon.com/addressing-inp... #cybersecurity #sanitizeuserinput	2021-06-24 00:40:10
 @DanielTechIT	hackernoon: "Addressing Input Sanitization Bugs and CVE 2021-21321" hackernoon.com/addressing-inp... #cybersecurity #sanitizeuserinput	2021-06-24 07:13:51
 @hackernoon	"Addressing Input Sanitization Bugs and CVE 2021-21321" hackernoon.com/addressing-inp... #cybersecurity #sanitizeuserinput	2021-06-30 18:24:22
 @hackernoon	"Addressing Input Sanitization Bugs and CVE 2021-21321" hackernoon.com/addressing-inp... #cybersecurity #sanitizeuserinput	2021-07-23 21:00:07
 @DanielTechIT	hackernoon: "Addressing Input Sanitization Bugs and CVE 2021-21321" hackernoon.com/addressing-inp... #cybersecurity #sanitizeuserinput	2021-07-24 07:12:36

© [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](#)