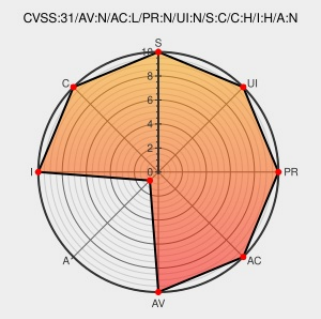
CVE-2021-21322

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

Last Modified on: 03/23/2021 11:28:59 PM UTC

CVE-2021-21322 - advisory for GHSA-c4qr-gmr9-v23w

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



Certain versions of Fastify-http-proxy from Fastify-http-proxy Project contain the following vulnerability:

fastify-http-proxy is an npm package which is a fastify plugin for proxying your http requests to another server, with hooks. 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 4.3.1.

CVE-2021-21322 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **fastify** - **fastify-http-proxy** version **< 4.3.1**

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

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	Tags	Link

Description	Tags	Link
Prefix escape · Advisory · fastify/fastify-http-proxy · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/fastify/fastify-http-proxy/security/advisories/GHSA-c4qr-gmr9-v23w
Merge pull request from GHSA-c4qr-gmr9-v23w · fastify/fastify-http-proxy@02d9b43 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/fastify/fastify-http-proxy/commit/02d9b43c770aa16bc44470edecfaeb7c17985016
fastify-http-proxy - npm	Product Third Party Advisory www.npmjs.com text/html	MISC www.npmjs.com/package/fastify-http-proxy

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

982931 Nodejs (npm) Security Update for fastify-http-proxy (GHSA-c4qr-gmr9-v23w)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastify-http-proxy Project	Fastify-http-proxy	All	All	All	All
Application	Fastify-http-proxy Project	Fastify-http-proxy	All	All	All	All

cpe:2.3:a:fastify-http-proxy_project:fastify-http-proxy:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:fastify-http-proxy_project:fastify-http-proxy:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→