



CVE-2022-24863

Published on: Not Yet Published

Last Modified on: 04/27/2022 01:31:00 PM UTC

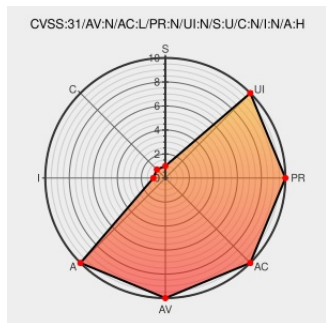
CVE-2022-24863 - advisory for GHSA-xg75-q3q5-cqmv

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

http-swagger is an open source wrapper to automatically generate RESTful API documentation with Swagger 2.0. In versions of http-swagger prior to 1.2.6 an attacker may perform a denial of service attack consisting of memory exhaustion on the host system. The cause of the memory exhaustion is down to improper handling of http methods. Users are advised to upgrade. Users unable to upgrade may to restrict the path prefix to the "GET" method as a workaround.

CVE-2022-24863 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [swaggo](#) - [http-swagger](#) version < 1.2.6

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: **7.8 - HIGH**

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

CVE References

Description	Tags	Link				
DOS in HTTP · Advisory · swaggo/http-swagger · GitHub	github.com text/html	CONFIRM github.com/swaggo/http-swagger/security/advisories/GHSA-xg75-q3q5-cqmv				
fix: security improvement (#62) · swaggo/http-swagger@b7d83e8 · GitHub	github.com text/html	MISC github.com/swaggo/http-swagger/commit/b7d83e8fba85a7a51aa7e45e8244b4173f15049e				
Release v1.2.6 · swaggo/http-swagger · GitHub	github.com text/html	MISC github.com/swaggo/http-swagger/releases/tag/v1.2.6				
fix: security improvement by ubogdan · Pull Request #62 · swaggo/http-swagger · GitHub	github.com text/html	MISC github.com/swaggo/http-swagger/pull/62				
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	Http-swagger Project	Http-swagger	All	All	All	All
cpe:2.3:a:http-swagger_project:http-swagger:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
@CVEreport	CVE-2022-24863 : http-swagger is an open source wrapper to automatically generate RESTful API documentation with Sw... twitter.com/i/web/status/1...					2022-04-18 19:05:40
@0xGaurav	cve.report/CVE-2022-24863					2022-04-18 19:09:09
/r/netcve	CVE-2022-24863					2022-04-18 19:38:37
← Previous ID			Next ID →			