



CVE-2021-43855

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-43855
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-27 18:15:00 UTC
Updated	2022-01-07 14:01:00 UTC
Description	Wiki.js is a wiki app built on node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through a SVG file upload.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Requarks	Wiki.js	All	All	All	All

References

Reference	Source	Link	Tags
Stored XSS via SVG file upload with fake MIME type · Advisory · Requarks/wiki · GitHub	CONFIRM	github.com	
fix: validate svg file extension in addition to client mime type · Requarks/wiki@57b56d3 · GitHub	MISC	github.com	
Release 2.5.264 · Requarks/wiki · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report