



CVE-2021-25993

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

Summary

CVE	CVE-2021-25993
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-29 17:15:00 UTC
Updated	2022-01-06 20:38:00 UTC
Description	In Requarks wiki.js, versions 2.0.0-beta.147 to 2.5.255 are affected by Stored XSS vulnerability, where a low privileged (edi

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	2.0.0	beta147	All	All
Application	Requarks	Wiki.js	2.0.0	beta148	All	All
Application	Requarks	Wiki.js	2.0.0	beta174	All	All
Application	Requarks	Wiki.js	2.0.0	beta180	All	All
Application	Requarks	Wiki.js	2.0.0	beta203	All	All
Application	Requarks	Wiki.js	2.0.0	beta208	All	All
Application	Requarks	Wiki.js	2.0.0	beta230	All	All
Application	Requarks	Wiki.js	2.0.0	beta241	All	All
Application	Requarks	Wiki.js	2.0.0	beta267	All	All
Application	Requarks	Wiki.js	2.0.0	beta268	All	All
Application	Requarks	Wiki.js	2.0.0	beta275	All	All
Application	Requarks	Wiki.js	2.0.0	beta303	All	All
Application	Requarks	Wiki.js	2.0.0	rc1	All	All
Application	Requarks	Wiki.js	2.0.0	rc17	All	All
Application	Requarks	Wiki.js	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2021-25993 WhiteSource Vulnerability Database	MISC	www.whitesourcesoftware.com	
fix: sanitize SVG uploads · Requarks/wiki@5d3e814 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: WhiteSource Vulnerability Research Team (WVR)

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

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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