



CVE-2023-26487

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

Summary

CVE	CVE-2023-26487
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-04 00:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. `lassoAppend` is a function that appends a new element to the end of an array. It takes a string as input and returns a new array with the string added to the end. This function is vulnerable to a cross-site scripting (XSS) attack because it does not sanitize the input. An attacker can inject malicious code into the array, which will be executed when the array is rendered. This can lead to the theft of sensitive information or the execution of arbitrary code on the user's browser.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vega-functions Project	Vega-functions	All	All	All	All
Application	Vega Project	Vega	All	All	All	All

References

Reference	Source	Link	Tags
Release v5.23.0 · vega/vega · GitHub	MISC	github.com	
fix: lassoAppend XSS w/typecheck + array spread instead of push · vega/vega@01adb03 · GitHub	MISC	github.com	
XSS vulnerability in `lassoAppend` function · Advisory · vega/vega · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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