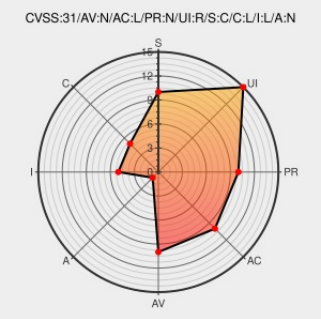
CVE-2023-22461

Published on: Not Yet Published

Last Modified on: 01/10/2023 07:14:00 PM UTC

CVE-2023-22461 - advisory for GHSA-h857-2g56-468g

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



Certain versions of Sanitize-svg from Sanitize-svg Project contain the following vulnerability:

The `sanitize-svg` package, a small SVG sanitizer to prevent cross-site scripting attacks, uses a deny-list-pattern to sanitize SVGs to prevent XSS. In doing so, literal `<script>`-tags and on-event handlers were detected in versions prior to 0.4.0. As a result, downstream software that relies on `sanitize-svg` and expects resulting SVGs to be safe, may be vulnerable to cross-site scripting. This vulnerability was addressed in v0.4.0. There are no known workarounds

CVE-2023-22461 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **mattkrick** - **sanitize-svg** version **= < 0.4**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Merge pull request from GHSA-h857-2g56-468g · mattkrick/sanitize-svg@b107e45 · GitHub	github.com text/html	MISC github.com/mattkrick/sanitize-svg/commit/b107e453ede7b58adcccae74a3e474c012eec85d
Filter Bypass Allows Cross-Site Scripting (XSS) · Advisory · mattkrick/sanitize-svg · GitHub	github.com text/html	MISC github.com/mattkrick/sanitize-svg/security/advisories/GHSA-h857-2g56-468g

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	Sanitize-svg Project	Sanitize-svg	All	All	All	All

cpe:2.3:a:sanitize-svg_project:sanitize-svg:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-22461 : The `sanitize-svg` package, a small SVG sanitizer to prevent cross-site scripting attacks, uses a… twitter.com/i/web/status/1…	2023-01-04 15:07:24

← Previous ID

Next ID→