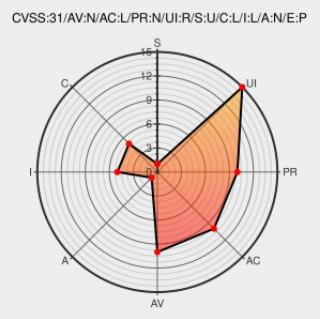
CVE-2021-23784

Published on: 11/03/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 09:38:18 PM UTC

CVE-2021-23784

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



Certain versions of Tempura from Tempura Project contain the following vulnerability:

This affects the package tempura before 0.4.0. If the input to the esc function is of type object (i.e an array) it is returned without being escaped/sanitized, leading to a potential Cross-Site Scripting vulnerability.

CVE-2021-23784 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Release v0.4.0 · lukeed/tempura · GitHub	github.com text/html	MISC github.com/lukeed/tempura/releases/tag/v0.4.0
break: ensure `esc` always returns a string; · lukeed/tempura@58a5c36 ·	github.com text/html	MISC github.com/lukeed/tempura/commit/58a5c3671e2f36b26810e77ead9e0dd471902f9b

GitHub

Cross-site Scripting (XSS) in tempura | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-TEMPURA-1569633

Related QID Numbers

980208 Nodejs (npm) Security Update for tempura (GHSA-w4v7-hwx7-9929)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tempura Project	Tempura	All	All	All	All

cpe:2.3:a:tempura_project:tempura:*:*:*:*:*:*:*:*:

Discovery Credit

Alessio Della Libera of Snyk Research Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23784 : This affects the package tempura before 0.4.0. If the input to the esc function is of type object… twitter.com/i/web/status/1…	2021-11-03 17:33:02

← Previous ID

Next ID→