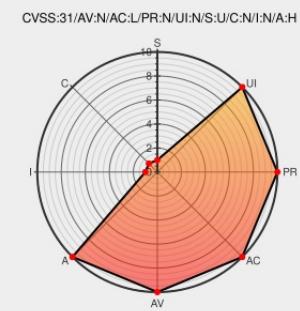
CVE-2023-26132

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:09:00 AM UTC

CVE-2023-26132

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



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

Versions of the package dottie before 2.0.4 are vulnerable to Prototype Pollution due to insufficient checks, via the set() function and the current variable in the /dottie.js file.

CVE-2023-26132 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Prototype Pollution in dottie | CVE-2023-26132 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-DOTTIE-3332763
dottie.js/dottie.js at b48e22714aae4489ea6276452f22cc61980ba5a4 · mickhansen/dottie.js · GitHub	github.com text/html	MISC github.com/mickhansen/dottie.js/blob/b48e22714aae4489ea6276452f22
rudimentary __proto__ guarding · mickhansen/dottie.js@7d3aee1 · GitHub	github.com text/html	MISC github.com/mickhansen/dottie.js/commit/7d3aee1c9c3c84272(

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:dottie_project:dottie:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→