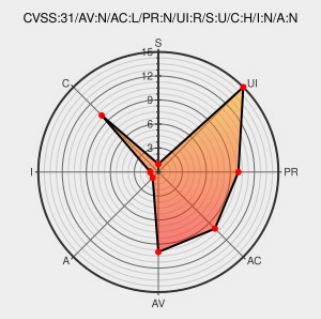
CVE-2020-7770

Published on: 11/12/2020 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:44:00 PM UTC

CVE-2020-7770

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



Certain versions of Json8 from Json8 Project contain the following vulnerability:

This affects the package json8 before 1.0.3. The function adds in the target object the property specified in the path, however it does not properly check the key being set, leading to a prototype pollution.

CVE-2020-7770 has been assigned by report@snyk.io to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
json8-merge-patch: Prevent prototype pollution 2 (#116) · sonnyp/JSON8@2e89026 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/sonnyp/JSON8/commit/2e890261b66cbc54ae01d0c79c71b0fd18379e7e

Prototype Pollution in json8 | Snyk	Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-JSON8-1017116

Related QID Numbers

982608 Nodejs (npm) Security Update for json8 (GHSA-7h43-gx24-p529)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Json8 Project	Json8	All	All	All	All
Application	Json8 Project	Json8	All	All	All	All

cpe:2.3:a:json8_project:json8:*:*:*:*:*:*:*:*:

cpe:2.3:a:json8_project:json8:*:*:*:*:*:*:*:*:

Discovery Credit

Alessio Della Libera (d3lla)

← Previous ID

Next ID→