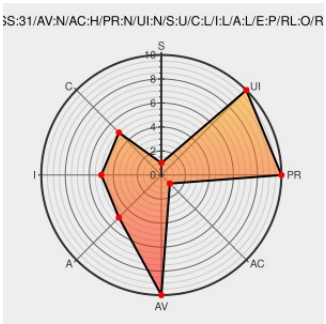
CVE-2021-23509

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

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

CVE-2021-23509

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



Certain versions of Json-ptr from Json-ptr Project contain the following vulnerability:

This affects the package json-ptr before 3.0.0. A type confusion vulnerability can lead to a bypass of CVE-2020-7766 when the user-provided keys used in the pointer parameter are arrays.

CVE-2021-23509 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
Prototype Pollution in json-ptr | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-JSONPTR-1577291
GitHub - flitbit/json-ptr: A complete implementation of JSON Pointer (RFC 6901) for nodejs and modern browsers.	github.com text/html	MISC github.com/flitbit/json-ptr%23security-vulnerabilities-resolved

Vulnerability fix and packaging rollup by cerebralkungfu · Pull Request #42 · flitbit/json-ptr · GitHub	github.com text/html	MISC github.com/flitbit/json-ptr/pull/42
Fixed vulnerability reported by Snyk · flitbit/json-ptr@5dc458f · GitHub	github.com text/html	MISC github.com/flitbit/json-ptr/commit/5dc458fbad1c382a2e3ca6d62e66ede3d92849ca
Prototype Pollution in org.webjars.npm:json-ptr | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1767165

Related QID Numbers

980210 Nodejs (npm) Security Update for json-ptr (GHSA-8gwj-8hxc-285w)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Json-ptr Project	Json-ptr	All	All	All	All

cpe:2.3:a:json-ptr_project:json-ptr:*:*:*:*:*:*:*:*:

Discovery Credit

Alessio Della Libera of Snyk Research Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23509 : This affects the package json-ptr before 3.0.0. A type confusion vulnerability can lead to a bypa… twitter.com/i/web/status/1…	2021-11-03 17:32:33

← Previous ID

Next ID→