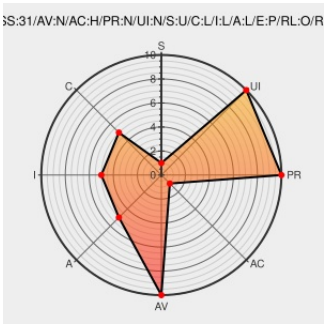
CVE-2021-23807

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

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

CVE-2021-23807

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



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

This affects the package jsonpointer before 5.0.0. A type confusion vulnerability can lead to a bypass of a previous Prototype Pollution fix when the pointer components are arrays.

CVE-2021-23807 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
Invalid vulnerability	snyk.io text/html Inactive Link Not Archived	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1910273
Merge pull request #51 from	github.com	MISC github.com/janl/node-

dellalibera/fix-prototype-pollution · janl/node-jsonpointer@a0345f3 · GitHub	text/html	jsonpointer/commit/a0345f3550cd9c4d89f33b126390202b89510ad4
fix-prototype-pollution by dellalibera · Pull Request #51 · janl/node-jsonpointer · GitHub	github.com text/html	MISC github.com/janl/node-jsonpointer/pull/51
Prototype Pollution in jsonpointer | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-JSONPOINTER-1577288

Related QID Numbers

905109 Common Base Linux Mariner (CBL-Mariner) Security Update for reaper (12624)

980209 Nodejs (npm) Security Update for jsonpointer (GHSA-282f-qqgm-c34q)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:jsonpointer_project:jsonpointer:*:*:*:*:*:node.js:*:*:

Discovery Credit

Alessio Della Libera of Snyk Research Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23807 : This affects the package jsonpointer before 5.0.0. A type confusion vulnerability can lead to a b… twitter.com/i/web/status/1…	2021-11-03 17:33:32
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-23807 Description: This affects the package jsonpointer before 5.0.0. A… twitter.com/i/web/status/1…	2021-11-03 19:00:11
@threatmeter	jsonpointer up to 5.0.0 code injection [CVE-2021-23807] A vulnerability classified as critical was found in jsonpoi… twitter.com/i/web/status/1…	2021-11-04 07:51:10

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report